

Multi-Stage Robust Chinese Remainder Theorem

Li Xiao*, Xiang-Gen Xia*, and Wenjie Wang[†]

Abstract

It is well-known that the traditional Chinese remainder theorem (CRT) is not robust in the sense that a small error in a remainder may cause a large error in the reconstruction solution. A robust CRT was recently proposed for a special case when the greatest common divisor (gcd) of all the moduli is more than 1 and the remaining integers factorized by the gcd of all the moduli are co-prime. In this special case, a closed-form reconstruction from erroneous remainders was proposed and a necessary and sufficient condition on the remainder errors was obtained. It basically says that the reconstruction error is upper bounded by the remainder error level τ if τ is smaller than a quarter of the gcd of all the moduli. In this paper, we consider the robust reconstruction problem for a general set of moduli. We first present a necessary and sufficient condition for the remainder errors for a robust reconstruction from erroneous remainders with a general set of moduli and also a corresponding robust reconstruction method. This can be thought of as a single stage robust CRT. We then propose a two-stage robust CRT by grouping the moduli into several groups as follows. First, the single stage robust CRT is applied to each group. Then, with these robust reconstructions from all the groups, the single stage robust CRT is applied again across the groups. This is then easily generalized to multi-stage robust CRT. Interestingly, with this two-stage robust CRT, the robust reconstruction holds even when the remainder error level τ is above the quarter of the gcd of all the moduli. In this paper, we also propose an algorithm on how to group a set of moduli for a better reconstruction robustness of the two-stage robust CRT in some special cases.

Index Terms

Chinese remainder theorem, robustness, frequency estimation from undersamplings, greatest common divisor, moduli

I. INTRODUCTION

The problem of reconstructing a large integer from its several remainders modulo several smaller positive integers (called moduli) may occur in many applications, such as phase unwrapping in radar signal processing [10], [14]–[23] and frequency determination from several undersampled waveforms [8], [9]. The traditional solution for this problem is the Chinese remainder theorem (CRT), see for example, [1], [2], that uniquely formulates the solution from the remainders if all the moduli are co-prime and the large integer is less than the product of all

*Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 U.S.A. (e-mail: {lixiao, xxia}@ee.udel.edu). Their work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-12-1-0055.

[†]School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, China (e-mail: wjwang@xjtu.edu.cn). His work was supported in part by the Natural Science Foundation of China (NSFC) No. 60971113.

the moduli. When the moduli are not co-prime, the large integer can be uniquely determined if it is less than the least common multiple (lcm) of all the moduli [3], [4], where one may also find the reconstruction methods. However, it is well-known that the above solution is not robust in the sense that a small error in a remainder may cause a large error in the reconstruction solution, which may degrade the performance of its applications in phase unwrapping and frequency determination, since in these applications, signals are usually noisy and the detected remainders may be erroneous. For the robustness, there have been several studies recently [11]–[13]. Robust reconstructions from erroneous remainders were recently proposed in [12], [13] for a special case when the greatest common divisor (gcd) of all the moduli is more than 1 and the remaining integers factorized by the gcd of all the moduli are co-prime. In this special case, a closed-form reconstruction from erroneous remainders was proposed in [13] and a necessary and sufficient condition on the remainder errors was also obtained in [13]. It basically says that the reconstruction error is upper bounded by the remainder error level τ if τ is smaller than a quarter of the gcd of all the moduli [12]. A special version of this result was obtained earlier in [10]. In some applications, an unknown, such as the phase unwrapping and frequency estimation, is real valued in general. So, in [13] the closed-form robust CRT algorithm was naturally generalized to real numbers. Also, a lattice based method was proposed in [25] to address the problem of estimating a real unknown distance with a closed-form algorithm using phase measurements taken at multiple co-prime wavelengths. One can see that there are constraints on the moduli in previous works. The constraints on the moduli may, however, limit the robustness when the range (called dynamic range) of the determinable integers is roughly fixed.

Different from robustly reconstructing the large integer from its erroneous remainders, another existing approach is to accurately determine the large integer by using some of the error-free remainders among all the remainders [5], [6], [9], which may require that significantly many remainders are error-free and a large number of moduli/remainders may be needed. This approach may sacrifice the dynamic range for a given set of moduli (or undersampling rates [9]) and furthermore, in some signal processing applications, to obtain error-free remainders may not be even possible, because observed signals are usually noisy. A probabilistic approach to deal with noises in CRT was proposed in [7], where all the moduli are required to be primes.

In this paper, we consider the robust reconstruction problem for a general set of moduli on which the constraint used in [12], [13] is no longer required. We first present a necessary and sufficient condition for the remainder errors for a robust reconstruction from erroneous remainders with a general set of moduli, where a reconstruction method is also proposed. This can be thought of as a single stage robust CRT. We then propose a two-stage robust CRT by grouping the moduli into several smaller groups as follows. First, the robust single stage CRT is applied to each group. Then, with these robust reconstructions from all the groups, the robust single stage CRT is applied again across the groups. Interestingly, with this two-stage robust CRT, the robust reconstruction holds even when the remainder error level τ is above the quarter of the gcd of all the moduli. The two-stage robust CRT is then easily generalized to multi-stage robust CRT. In this paper, we also propose an algorithm on how to group a set of moduli for the better reconstruction robustness of the two-stage robust CRT in some special cases.

Note that the two-stage robust CRT is first appeared in [24] that is, however, based on the special single stage robust CRT in [13] when the remaining factors of all the moduli after factorizing out their gcd are co-prime. With the two-stage robust CRT obtained in [24], the remainder error level τ is, in fact, not better than the quarter

of the gcd of all the moduli. In contrast, our newly proposed two-stage or multi-stage robust CRT in this paper is based on the generalized single stage robust CRT for arbitrary moduli also newly obtained in this paper and as mentioned earlier, the remainder error level τ can be above the quarter of the gcd of all the moduli, i.e., it achieves a better robustness bound than [24] does.

This paper is organized as follows. In Section II, we first briefly introduce the robust CRT results obtained in [12], [13]. We then propose our new single stage robust CRT with the necessary and sufficient condition for a general set of moduli. In Section III, we propose two-stage and multi-stage robust CRT. In Section IV, we propose an algorithm on how to group a set of moduli for a better reconstruction robustness of the two-stage robust CRT. In Section V, we present some simulation results on estimating integers with a general set of moduli. In Section VI, we conclude this paper.

II. SINGLE STAGE ROBUST CRT

Let us first see the robust remaindering problem. Let N be a positive integer, $0 < M_1 < M_2 < \dots < M_L$ be L moduli, and r_1, r_2, \dots, r_L be the L remainders of N , i.e.,

$$N \equiv r_i \pmod{M_i} \text{ or } N = n_i M_i + r_i, \quad (1)$$

where $0 \leq r_i < M_i$ and n_i is an unknown integer, for $1 \leq i \leq L$. It is not hard to see that N can be uniquely reconstructed from its L remainders r_i if and only if $0 \leq N < \text{lcm}(M_1, M_2, \dots, M_L)$. If all the moduli M_i are co-prime, then the Chinese Remainder Theorem (CRT) provides a simple reconstruction formula [1], [2].

The problem we are interested in this paper is how to robustly reconstruct N when the remainders r_i have errors:

$$0 \leq \tilde{r}_i \leq M_i - 1 \text{ and } |\tilde{r}_i - r_i| \leq \tau, \quad (2)$$

where τ is an error level that may be determined by, for example, the signal-to-noise ratio (SNR) and is also called remainder error bound. Now we want to reconstruct N from these erroneous remainders \tilde{r}_i and the known moduli M_i . The basic idea for the robust CRT in the recent studies and also this paper is to accurately determine the unknown integers n_i in (1) which are the folding numbers that may cause large errors in the reconstructions if they are erroneous. Therefore, the problem is to correctly determine the folding numbers n_i from these erroneous remainders \tilde{r}_i .

Once n_i for $1 \leq i \leq L$ are correctly found, an estimate of N can be given by

$$\hat{N}(i) = n_i M_i + \tilde{r}_i = n_i M_i + r_i + \Delta r_i, \text{ for any } i, \ 1 \leq i \leq L, \quad (3)$$

where $\Delta r_i = \tilde{r}_i - r_i$ denote the errors of the remainders. From (2), $|\Delta r_i| \leq \tau$. Then, an estimate of the unknown parameter N is the average of $\hat{N}(i)$:

$$\begin{aligned} \hat{N} &= \left[\frac{1}{L} \sum_{i=1}^L \hat{N}(i) \right] \\ &= N + \left[\frac{1}{L} \sum_{i=1}^L \Delta r_i \right] \\ &= N + \Delta \bar{r}, \end{aligned} \quad (4)$$

where $\Delta\bar{r}$ is the average of the remainder errors, and $[\cdot]$ stands for the rounding integer, i.e., for any $x \in \mathbb{R}$ (the set of all reals), $[x]$ is an integer and subject to

$$-\frac{1}{2} \leq x - [x] < \frac{1}{2}. \quad (5)$$

Clearly in this way the error of the above estimate of N is upper bounded by

$$|\hat{N} - N| \leq \tau, \quad (6)$$

i.e., \hat{N} is a robust estimate of N .

For the above robust remaindering problem, solutions, i.e., robust reconstruction algorithms, have been proposed in [12], [13] for a special case when the gcd of all the moduli is more than 1 and the remaining integers factorized by the gcd of all the moduli are co-prime. The main results can be briefly described below.

Let M be the gcd of all the moduli M_i in (1). Then $M_i = M\Gamma_i$, $1 \leq i \leq L$, and assume that all Γ_i for $1 \leq i \leq L$ are co-prime, i.e., the gcd of any pair Γ_i and Γ_j for $i \neq j$ is 1. Define $\Gamma \triangleq \Gamma_1\Gamma_2 \cdots \Gamma_L$. For $1 \leq i \leq L$, let

$$\gamma_i \triangleq \Gamma_1 \cdots \Gamma_{i-1}\Gamma_{i+1} \cdots \Gamma_L = \Gamma/\Gamma_i, \quad (7)$$

where $\gamma_1 \triangleq \Gamma_2 \cdots \Gamma_L$ and $\gamma_L \triangleq \Gamma_1 \cdots \Gamma_{L-1}$. We now show how to accurately determine the folding numbers n_i in [12] and [13], respectively. First, define

$$S_i \triangleq \left\{ (\bar{n}_1, \bar{n}_i) = \arg \min_{\substack{\bar{n}_1=0,1,\dots,\gamma_1-1 \\ \bar{n}_i=0,1,\dots,\gamma_i-1}} |\hat{n}_i M_i + \tilde{r}_i - \hat{n}_1 M_1 - \tilde{r}_1| \right\}. \quad (8)$$

Let $S_{i,1}$ denote the set of all the first components \bar{n}_1 of the pairs (\bar{n}_1, \bar{n}_i) in set S_i , i.e.,

$$S_{i,1} \triangleq \{ \bar{n}_1 | (\bar{n}_1, \bar{n}_i) \in S_i \text{ for some } \bar{n}_i \} \quad (9)$$

and define

$$S \triangleq \bigcap_{i=2}^L S_{i,1}. \quad (10)$$

It is proved in [12] that if the remainder error bound τ is smaller than a quarter of M , i.e., $\tau < M/4$, the folding numbers n_i for $1 \leq i \leq L$ can be accurately determined from S and S_i . Set S defined above contains only one element n_1 , and furthermore if $(n_1, \bar{n}_i) \in S_i$, then $\bar{n}_i = n_i$. In addition, [12] has proposed a 1-D searching method with the order of $2(L-1)\Gamma_i$ searches. When L or Γ_i gets large, the searching complexity is still high. Then, a closed-form robust CRT algorithm and its necessary and sufficient condition for it to hold have been proposed in [13]. For the closed-form algorithm, we refer the reader to [13] with which the following necessary and sufficient condition for the accurate determination of the folding numbers n_i is obtained in [13].

Proposition 1: [13] Assume that all Γ_i , for $1 \leq i \leq L$ are co-prime and

$$0 \leq N < \text{lcm}(M_1, M_2, \dots, M_L) = M\Gamma_1\Gamma_2 \cdots \Gamma_L. \quad (11)$$

Then, with the closed-form algorithm determining \hat{n}_i for $1 \leq i \leq L$ in [13], $\hat{n}_i = n_i$ for $1 \leq i \leq L$, i.e., the folding numbers n_i for $1 \leq i \leq L$ can be accurately determined, if and only if

$$-M/2 \leq \Delta r_i - \Delta r_1 < M/2, \text{ for all } 2 \leq i \leq L. \quad (12)$$

Although the condition (12) in Proposition 1 is necessary and sufficient for the uniqueness of the solution of the folding numbers n_i , it involves with two remainder errors and is hard to check in practice. However, with this result the following proposition becomes obvious, which coincides with the much simpler sufficient condition in [12].

Proposition 2: [12], [13] Assume that all Γ_i for $1 \leq i \leq L$ are co-prime and

$$0 \leq N < \text{lcm}(M_1, M_2, \dots, M_L) = M\Gamma_1\Gamma_2 \cdots \Gamma_L. \quad (13)$$

If the remainder error bound τ satisfies

$$\tau < M/4, \quad (14)$$

then we have $\hat{n}_i = n_i$ for $1 \leq i \leq L$, i.e., the folding numbers n_i for $1 \leq i \leq L$ can be accurately determined.

As it was mentioned earlier, these robust reconstruction results are based on the assumption that the gcd M of all the moduli is more than 1 and the remaining integers Γ_i in the moduli M_i factorized by their gcd M are co-prime. For example, $M_1 = 5 \cdot 5 = 25$, $M_2 = 5 \cdot 7 = 35$, $M_3 = 5 \cdot 16 = 80$, and $M_4 = 5 \cdot 19 = 95$, where $M = 5$. When the remainder error level $\tau < 5/4$, any integer less than $5 \cdot 5 \cdot 7 \cdot 16 \cdot 19$ can be reconstructed within the same error level as the remainders from the erroneous remainders by using the algorithms in [12], [13]. A natural question is what will happen if a general set of moduli M_i are used. For example, what will happen if $M_1 = 5 \cdot 14 = 70$, $M_2 = 5 \cdot 15 = 75$, $M_3 = 5 \cdot 16 = 80$, and $M_4 = 5 \cdot 18 = 90$? First of all, their gcd is $M = 5$ and if we divide them by their gcd, we get $\Gamma_1 = 14$, $\Gamma_2 = 15$, $\Gamma_3 = 16$, and $\Gamma_4 = 18$ and clearly these four Γ_i are not co-prime. So, we can not apply the algorithms or results in [12], [13] directly, which may limit the applications in practice.

We next propose an accurate determination algorithm for the folding numbers n_i from erroneous remainders for a general set of moduli M_i with a new necessary and sufficient condition on the remainder errors. Let us first see an algorithm for n_i .

Following the algorithm in [13], we can generalize the results as follows. First, from (1) we can equivalently write it as the following system of congruences:

$$\begin{cases} N = n_1 M_1 + r_1 \\ N = n_2 M_2 + r_2 \\ \vdots \\ N = n_L M_L + r_L. \end{cases} \quad (15)$$

We want to determine n_i for $1 \leq i \leq L$. To do so, we let the last $L - 1$ equations in (15) subtract the first one and we then have

$$\begin{cases} n_1 M_1 - n_2 M_2 = r_2 - r_1 \\ n_1 M_1 - n_3 M_3 = r_3 - r_1 \\ \vdots \\ n_1 M_1 - n_L M_L = r_L - r_1. \end{cases} \quad (16)$$

Next, denote

$$m_{1i} = \text{gcd}(M_1, M_i), \quad \Gamma_{1i} = \frac{M_1}{m_{1i}}, \quad \Gamma_{i1} = \frac{M_i}{m_{1i}}, \quad \text{and} \quad q_{i1} = \frac{r_i - r_1}{m_{1i}}.$$

Then, we can equivalently express equation (16) again as

$$\begin{cases} n_1\Gamma_{12} - n_2\Gamma_{21} = q_{21} \\ n_1\Gamma_{13} - n_3\Gamma_{31} = q_{31} \\ \vdots \\ n_1\Gamma_{1L} - n_L\Gamma_{L1} = q_{L1}. \end{cases} \quad (17)$$

Since Γ_{1i} and Γ_{i1} are co-prime, by Bézout's lemma (Lemma 1 in [13]) we get

$$\begin{cases} n_1 = q_{i1}\bar{\Gamma}_i + kq_{i1}\Gamma_{i1} \\ n_i = \frac{q_{i1}(\bar{\Gamma}_i\Gamma_{1i}-1)}{\Gamma_{i1}} + kq_{i1}\Gamma_{1i}, \end{cases} \quad (18)$$

where $1 \leq i \leq L$, $k \in \mathbb{Z}$ (the set of integers) and $\bar{\Gamma}_i$ is the modular multiplicative inverse of Γ_{1i} modulo Γ_{i1} .

We can use

$$\hat{q}_{i1} = \left\lfloor \frac{\tilde{r}_i - \tilde{r}_1}{m_{1i}} \right\rfloor = q_{i1} + \left\lfloor \frac{\Delta r_i - \Delta r_1}{m_{1i}} \right\rfloor \quad (19)$$

as an estimate of q_{i1} for $2 \leq i \leq L$. Recall that $\lfloor \cdot \rfloor$ stands for the rounding integer which is defined in (5). Let \hat{n}_i for $1 \leq i \leq L$ be a set of solutions of (17) when q_{i1} is replaced by \hat{q}_{i1} for $2 \leq i \leq L$. In summary, we have the following algorithm.

- **Step 1:** Calculate these values of $m_{1i} = \gcd(M_1, M_i)$, $\Gamma_{1i} = \frac{M_1}{m_{1i}}$ and $\Gamma_{i1} = \frac{M_i}{m_{1i}}$ for $2 \leq i \leq L$ from the given moduli M_j for $1 \leq j \leq L$, which can be done in advance.
- **Step 2:** Calculate \hat{q}_{i1} for $2 \leq i \leq L$ in (19) from the given erroneous remainders \tilde{r}_i for $1 \leq i \leq L$.
- **Step 3:** Calculate the remainders of $\hat{q}_{i1}\bar{\Gamma}_i$ modulo Γ_{i1} , i.e.,

$$\hat{\xi}_{i1} \equiv \hat{q}_{i1}\bar{\Gamma}_i \pmod{\Gamma_{i1}} \quad (20)$$

for $2 \leq i \leq L$, where $\bar{\Gamma}_i$ is the modular multiplicative inverse of Γ_{1i} modulo Γ_{i1} and can be calculated in advance.

- **Step 4:** Calculate \hat{n}_1 from the following system of congruences:

$$\hat{n}_1 \equiv \hat{\xi}_{i1} \pmod{\Gamma_{i1}}, \text{ for } 2 \leq i \leq L, \quad (21)$$

where moduli Γ_{i1} may not be co-prime, which can be done by using the algorithms in, for example, [3], [4], and in [4], a multi-level decoding technique to reconstruct the large integer is proposed.

- **Step 5:** Calculate \hat{n}_i for $2 \leq i \leq L$:

$$\hat{n}_i = \frac{\hat{n}_1\Gamma_{1i} - \hat{q}_{i1}}{\Gamma_{i1}}. \quad (22)$$

With the above algorithm, we have the following necessary and sufficient condition result for a general set of moduli.

Theorem 1: Let M_i , $1 \leq i \leq L$, be L arbitrarily distinct positive integers as a given set of moduli and $0 \leq N < \text{lcm}(M_1, M_2, \dots, M_L)$. Then, $\hat{n}_i = n_i$ for all $1 \leq i \leq L$, i.e., the folding numbers n_i for $1 \leq i \leq L$ can be accurately determined, if and only if

$$-\gcd(M_1, M_i)/2 \leq \Delta r_i - \Delta r_1 < \gcd(M_1, M_i)/2, \quad \text{for all } 2 \leq i \leq L. \quad (23)$$

Proof: We first prove the sufficiency. Considering the condition in (23) and the estimate of q_{i1} in (19), from (5) for the definition of the operator $[\cdot]$ we have $\hat{q}_{i1} = q_{i1}$. Then, from equation (18), n_1 and $\hat{q}_{i1}\bar{\Gamma}_i$ have the same remainder modulo Γ_{i1} . Since \hat{q}_{i1} , $\bar{\Gamma}_i$ and Γ_{i1} are known, we can calculate $\hat{q}_{i1}\bar{\Gamma}_i \equiv \hat{\xi}_{i1} \pmod{\Gamma_{i1}}$. Thus, $n_1 \equiv \hat{\xi}_{i1} \pmod{\Gamma_{i1}}$ for $2 \leq i \leq L$, which form a system of simultaneous congruences as $\hat{n}_1 \equiv \hat{\xi}_{i1} \pmod{\Gamma_{i1}}$. In addition, since $n_1 M_1 \leq N < \text{lcm}(M_1, M_2, \dots, M_L)$, it is not hard to see that n_1 is less than $\text{lcm}(\Gamma_{21}, \Gamma_{31}, \dots, \Gamma_{L1})$. So, according to the algorithm about generalized CRT in [4], n_1 can be uniquely reconstructed by solving the above system, and $n_1 = \hat{n}_1$.

After n_1 is determined, we can obtain other integers n_i for $2 \leq i \leq L$ from equations (17) or (18). Therefore, $\hat{n}_i = n_i$ for $2 \leq i \leq L$. Hence, the sufficiency is proved.

We next prove the necessity. Assume that there exists at least one remainder that does not satisfy (23). For example, the j -th remainder \tilde{r}_j , $2 \leq j \leq L$, does not satisfy (23). This equivalently leads to $[(\Delta r_j - \Delta r_1) / m_{1j}] \neq 0$ and therefore $\hat{q}_{j1} \neq q_{j1}$. We then have the following two cases.

Case A: When $[(\Delta r_j - \Delta r_1) / m_{1j}] \neq k\Gamma_{j1}$ for any $k \in \mathbb{Z}$. We want to prove that the remainders of $\hat{q}_{j1}\bar{\Gamma}_j$ and $q_{j1}\bar{\Gamma}_j$ modulo Γ_{j1} are different. Assume $\hat{q}_{j1}\bar{\Gamma}_j$ and $q_{j1}\bar{\Gamma}_j$ have the same remainder modulo Γ_{j1} , i.e.,

$$\hat{q}_{j1}\bar{\Gamma}_j - q_{j1}\bar{\Gamma}_j = k\Gamma_{j1}, \text{ for some } k \in \mathbb{Z}. \quad (24)$$

Multiplying both sides of (24) by Γ_{1j} and considering $\Gamma_{1j}\bar{\Gamma}_j = 1 + k\Gamma_{j1}$ for some $k \in \mathbb{Z}$, we have

$$\hat{q}_{j1} - q_{j1} = k\Gamma_{j1}, \text{ for some } k \in \mathbb{Z}. \quad (25)$$

According to (19), we have

$$[(\Delta r_j - \Delta r_1) / m_{1j}] = k\Gamma_{j1}, \text{ for some } k \in \mathbb{Z}. \quad (26)$$

This contradicts with the assumption. Hence, the remainders of $\hat{q}_{j1}\bar{\Gamma}_j$ and $q_{j1}\bar{\Gamma}_j$ modulo Γ_{j1} are different, i.e., n_1 and \hat{n}_1 have different congruences. Thus, $n_1 \neq \hat{n}_1$.

Case B: For every $2 \leq i \leq L$, $[(\Delta r_i - \Delta r_1) / m_{1i}] = k\Gamma_{i1}$ for some $k \in \mathbb{Z}$ but there exists at least one j with $2 \leq j \leq L$ such that $[(\Delta r_j - \Delta r_1) / m_{1j}] \neq 0$, i.e., $\hat{q}_{j1} \neq q_{j1}$. From equation (19), we have $\hat{q}_{i1}\bar{\Gamma}_i \equiv q_{i1}\bar{\Gamma}_i \pmod{\Gamma_{i1}}$ for $2 \leq i \leq L$. Hence, from the first equation in (18) and according to the generalized CRT, n_1 can be uniquely reconstructed. Thus, from Steps 1-4 in the above algorithm, we have $\hat{n}_1 = n_1$.

However, since $\hat{q}_{j1} \neq q_{j1}$, from equations (17) or the second equation in (18) we have $n_j \neq \hat{n}_j$. This proves the necessity. ■

The above result involves with two remainder errors and is hard to check in practice. Let τ be the maximal remainder error level, i.e., $|\Delta r_i| = |\tilde{r}_i - r_i| \leq \tau$, for $1 \leq i \leq L$. Similar to Proposition 2, we can also present a simpler sufficient condition.

Corollary 1: Let M_i , $1 \leq i \leq L$, be L arbitrarily distinct positive integers as a given set of moduli and $0 \leq N < \text{lcm}(M_1, M_2, \dots, M_L)$. If the remainder error bound τ satisfies

$$\tau < \max_{1 \leq i \leq L} \min_{1 \leq j \neq i \leq L} \frac{\gcd(M_i, M_j)}{4}, \quad (27)$$

then, we have $\hat{n}_i = n_i$ for all $1 \leq i \leq L$, i.e., the folding numbers n_i for $1 \leq i \leq L$ can be accurately determined.

Proof: Recall that in the procedure of proving Theorem 1 we just arbitrarily selected the first equation in (15) to be a reference to be subtracted from the other equations to get (16). In fact, to improve the robustness through selecting a proper reference equation to differentiate, we can choose the index i such that $\min_j \gcd(M_i, M_j) \geq \min_j \gcd(M_l, M_j)$ for $l \neq i$. Without loss of generality, modulus M_1 satisfies

$$\max_{1 \leq i \leq L} \min_{1 \leq j \neq i \leq L} \frac{\gcd(M_i, M_j)}{4} = \min_{1 \leq j \neq 1 \leq L} \frac{\gcd(M_1, M_j)}{4}.$$

Then, we have $\tau < \gcd(M_1, M_i)/4$ for $i \neq 1$. Since τ is the maximal remainder error level, i.e., $|\Delta r_i| = |\tilde{r}_i - r_i| \leq \tau$, for $1 \leq i \leq L$, we can obtain

$$|\Delta r_i - \Delta r_1| < \gcd(M_1, M_i) / 2, \text{ for } 2 \leq i \leq L. \quad (28)$$

Clearly, equation (28) implies the sufficient condition (23) in Theorem 1. Hence, $\hat{n}_i = n_i$ for all $1 \leq i \leq L$. Therefore, we complete the proof. \blacksquare

Remark 1: Since in the above new result, there is no any constraint to the moduli M_i for $1 \leq i \leq L$, some of the moduli may be redundant with respect to the range $0 \leq N < \text{lcm}(M_1, M_2, \dots, M_L)$ of the determinable unknown integer N . The first case is when there exist a pair of moduli M_{i_1} and M_{i_2} such that $M_{i_1} = nM_{i_2}$ for $n \in \mathbb{N}$ (the set of all positive integers) and in this case M_{i_2} is redundant for the determinable range of N , i.e., the lcm of all M_i . The other case is when there exists one moduli M_{i_3} that is a factor of some other (more than one) moduli's lcm, i.e., $\text{lcm}(M_{i_4}, M_{i_5}, \dots, M_{i_k}) = nM_{i_3}$ for some $n \in \mathbb{N}$ and $k > 4$, and in this case M_{i_3} is redundant similarly. When a determinable range of N is fixed, we can add or delete some of the redundant moduli to or from the moduli set in order to get a better robustness bound for τ . For example, the redundant modulus 30 in moduli set $\{20, 45, 30\}$ improves the robustness bound compared with the robustness bound of moduli set $\{20, 45\}$ from $5/4$ to $10/4$. On the other hand, the redundant modulus 10 in $\{10, 45, 30\}$ with its robustness bound $10/4$ does not help but worsens the robustness bound compared with $15/4$ of $\{45, 30\}$, so it is better to delete the modulus 10 from the moduli set. Below is a general result.

Corollary 2: If there exist a pair of moduli M_{i_1} and M_{i_2} such that $M_{i_1} = nM_{i_2}$ for $n \in \mathbb{N}$, then, the redundant modulus M_{i_2} does not help to increase the robustness bound and it can be deleted from the set of moduli.

Proof: Without loss of generality, we can assume for a moduli set $\{M_1, M_2, \dots, M_L\}$ that $\gcd(M_1, M_2) \geq \gcd(M_1, M_3) \geq \dots \geq \gcd(M_1, M_L)$ and the robustness bound is

$$\max_{1 \leq i \leq L} \min_{1 \leq j \neq i \leq L} \frac{\gcd(M_i, M_j)}{4} = \frac{\gcd(M_1, M_L)}{4}.$$

Consider another set of moduli $\{M_1, M_2, \dots, M_L, M_{L+1}\}$ where M_{L+1} is a factor of one moduli M_q in $\{M_1, M_2, \dots, M_L\}$, i.e., $M_q = nM_{L+1}$ for $n \in \mathbb{N}$, $1 \leq q \leq L$. For the moduli $\{M_1, M_2, \dots, M_L, M_{L+1}\}$, its robustness bound is

$$\max_{1 \leq i \leq L+1} \min_{1 \leq j \neq i \leq L+1} \frac{\gcd(M_i, M_j)}{4}.$$

To calculate it, we split $1 \leq i \leq L+1$ into two parts: $1 \leq i \leq L$ and $i = L+1$. And,

$$\max_{1 \leq i \leq L+1} \min_{1 \leq j \neq i \leq L+1} \frac{\gcd(M_i, M_j)}{4} = \max \left\{ \underbrace{\max_{1 \leq i \leq L} \min_{1 \leq j \neq i \leq L+1} \frac{\gcd(M_i, M_j)}{4}}_A, \underbrace{\min_{1 \leq j \leq L} \frac{\gcd(M_{L+1}, M_j)}{4}}_B \right\}.$$

As for A , since

$$\min_{\substack{1 \leq j \neq i \leq L+1 \\ 1 \leq i \leq L}} \frac{\gcd(M_i, M_j)}{4} \leq \min_{\substack{1 \leq j \neq i \leq L \\ 1 \leq i \leq L}} \frac{\gcd(M_i, M_j)}{4},$$

we have

$$A \leq \max_{1 \leq i \leq L} \min_{1 \leq j \neq i \leq L} \frac{\gcd(M_i, M_j)}{4} = \frac{\gcd(M_1, M_L)}{4}.$$

As for B , since

$$\gcd(M_{L+1}, M_j) \leq \gcd(M_q, M_j) \text{ for } 1 \leq j \leq L,$$

we have

$$B \leq \min_{1 \leq j \neq q \leq L} \frac{\gcd(M_{L+1}, M_j)}{4} \leq \max_{1 \leq i \leq L} \min_{1 \leq j \neq i \leq L} \frac{\gcd(M_i, M_j)}{4} = \frac{\gcd(M_1, M_L)}{4}.$$

Thus, we can derive

$$\max_{1 \leq i \leq L+1} \min_{1 \leq j \neq i \leq L+1} \frac{\gcd(M_i, M_j)}{4} = \max\{A, B\} \leq \max_{1 \leq i \leq L} \min_{1 \leq j \neq i \leq L} \frac{\gcd(M_i, M_j)}{4} = \frac{\gcd(M_1, M_L)}{4}.$$

This tells us that the redundant modulus M_{L+1} does not help to increase the robustness bound of the set of moduli $\{M_1, M_2, \dots, M_L, M_{L+1}\}$ compared with that of $\{M_1, M_2, \dots, M_L\}$. \blacksquare

From the result of Corollary 2, for a set of moduli, we can delete this kind of redundant modulus M_{i_2} when there exists one modulus M_{i_1} in the moduli set such that $M_{i_1} = nM_{i_2}$. So, throughout this paper, a set of moduli we consider does not include such a pair of moduli in a single stage robust CRT.

From the above results, one can see that the choice of the reference remainder is important in determining the maximal possible robustness bound for τ when the whole moduli set of L arbitrary moduli is considered once as above. In fact, when the moduli satisfy the constraint, i.e., Γ_i are co-prime, in Proposition 2 in [12], [13], it has been pointed out and analyzed in [13] that a proper reference remainder indeed plays an important role in improving the performance in practice.

Going back to the necessary and sufficient condition (23), one can see that the remainder error difference bound depends on $\gcd(M_1, M_i)$, that varies with each M_i , and the choice of the reference modulus M_1 . This means that for the robust reconstruction of N , the error levels of its remainders \tilde{r}_i for different i may have different requirements. Also, as it was mentioned earlier, using M_1 as the reference modulus is not necessary. Let us choose the reference modulus M_k that satisfies

$$\min_{1 \leq j \neq k \leq L} \frac{\gcd(M_k, M_j)}{4} = \max_{1 \leq i \leq L} \min_{1 \leq j \neq i \leq L} \frac{\gcd(M_i, M_j)}{4}, \quad (29)$$

and the remainder error bound τ_k for the reference remainder r_k satisfy

$$|\Delta r_k| = |\tilde{r}_k - r_k| \leq \tau_k < \min_{1 \leq j \neq k \leq L} \frac{\gcd(M_k, M_j)}{4}. \quad (30)$$

Then, we have the following result.

Corollary 3: Let M_i , $1 \leq i \leq L$, be L arbitrarily distinct positive integers as a given set of moduli and $0 \leq N < \text{lcm}(M_1, M_2, \dots, M_L)$, define the remainder error bound for r_i as τ_i , i.e., $|\Delta r_i| = |\tilde{r}_i - r_i| \leq \tau_i$ for $1 \leq i \leq L$, and the reference modulus and its corresponding remainder error bound are M_k and τ_k satisfying (29) and (30) above for some k with $1 \leq k \leq L$. If the remainder error bound τ_i , $1 \leq i \neq k \leq L$, satisfies

$$|\Delta r_i| = |\tilde{r}_i - r_i| \leq \tau_i \leq \frac{\gcd(M_k, M_i)}{2} - \min_{1 \leq j \neq k \leq L} \frac{\gcd(M_k, M_j)}{4}, \quad (31)$$

then, we have $\hat{n}_i = n_i$ for all $1 \leq i \leq L$, i.e., the folding numbers n_i for $1 \leq i \leq L$ can be accurately determined.

Proof: If the reference modulus and its corresponding remainder error bound are M_k and τ_k , $1 \leq k \leq L$, we just need to prove $|\Delta r_i - \Delta r_k| < \gcd(M_i, M_k)/2$ for all $1 \leq i \neq k \leq L$, which implies the sufficient condition (23) in Theorem 1.

Since $|\Delta r_i| \leq \tau_i \leq \frac{\gcd(M_k, M_i)}{2} - \min_{1 \leq j \neq k \leq L} \frac{\gcd(M_k, M_j)}{4}$, we have

$$|\Delta r_i - \Delta r_k| \leq |\Delta r_i| + |\Delta r_k| \leq \tau_i + \tau_k < \frac{\gcd(M_k, M_i)}{2}. \quad (32)$$

Thus, Corollary 3 is proved. \blacksquare

Next, we consider the example mentioned before again.

Example 1: Let $M_1 = 5 \cdot 14 = 70$, $M_2 = 5 \cdot 15 = 75$, $M_3 = 5 \cdot 16 = 80$, and $M_4 = 5 \cdot 18 = 90$. It is easy to see that their gcd is $M = 5$, and $\{M_i\}_{i=1,2,3,4}$ do not satisfy the constraint of Propositions 1 and 2 in [12], [13]. Thus, their results can not be applied here. However, from the result of Corollary 1, we can obtain the maximal robustness bound τ for all remainders as $10/4$, which is even larger than $5/4$, a quarter of the gcd of all the moduli. From the result of Corollary 3, we choose M_4 as the reference modulus that does satisfy (29), and we can get the robustness bound for each remainder as follows: $\tau_1 \leq 10/4$, $\tau_2 \leq 20/4$, $\tau_3 \leq 10/4$ and $\tau_4 < 10/4$. One can see that, if we treat remainder error bounds individually as above, the remainder error bounds for some of the individual remainders, such as the second remainder in this example, may be larger than that in (27) in Corollary 1 for all the remainder error levels. In addition, the robust reconstruction range of N is also $0 \leq N < \text{lcm}(M_1, M_2, M_3, M_4)$.

It is clear that when moduli Γ_{i1} for $2 \leq i \leq L$ are co-prime similar to the case of [13], from the system of congruences (21) in Step 4 in the above algorithm, a closed-form single stage CRT can be obtained as [13] and we can replace Step 4 with the following Step 4*.

- **Step 4*:** Calculate \hat{n}_1 :

$$\hat{n}_1 = \sum_{i=2}^L \hat{\xi}_{i1} b_{i1} \frac{\gamma}{\Gamma_{i1}} \bmod \gamma, \quad (33)$$

where b_{i1} is the modular multiplicative inverse of γ/Γ_{i1} modulo Γ_{i1} , which can be calculated in advance, and $\gamma = \Gamma_{21}\Gamma_{31} \cdots \Gamma_{L1}$. After that, from (22) we can get the formulas for other \hat{n}_i for $2 \leq i \leq L$.

Next, let us consider the result in [24]. If we consider the following special case of moduli in Corollary 3, we can obtain a better result of the remainder error bounds than that in [24]. Let a set of moduli be

$$\{M_1, M_2, \dots, M_{L_1+L_2}\} = \{M\Gamma_{1,1}, M\Gamma_{1,2}, \dots, M\Gamma_{1,L_1}, MM'\Gamma_{2,1}, MM'\Gamma_{2,2}, \dots, MM'\Gamma_{2,L_2}\},$$

where $L_1 \geq 2$. Then, we have the following corollary.

Corollary 4: Assume that all the $\Gamma_{j,i}$, $1 \leq i \leq L_j$, $j = 1, 2$, are pair-wisely co-prime, let $\Gamma_{1,1} = \dot{\Gamma}_{1,1}M'$, where $\dot{\Gamma}_{1,1}$ is an integer, and $0 \leq N < \text{lcm}(M_1, M_2, \dots, M_{L_1+L_2})$. Denote τ_i as the error bound for each remainder r_i for $1 \leq i \leq L_1 + L_2$. If

$$\begin{aligned} |\Delta r_1| &\leq \tau_1 < M/4, \\ |\Delta r_i| &\leq \tau_i \leq M/4, \quad \text{for all } 2 \leq i \leq L_1, \\ |\Delta r_i| &\leq \tau_i \leq MM'/2 - M/4, \quad \text{for all } L_1 + 1 \leq i \leq L_1 + L_2, \end{aligned} \quad (34)$$

then with a closed-form algorithm we have $\hat{n}_i = n_i$ for $1 \leq i \leq L_1 + L_2$, i.e., the folding numbers n_i for $1 \leq i \leq L_1 + L_2$ can be accurately determined.

Proof: Since

$$\min_{1 \leq j \leq L_1 + L_2} \frac{\gcd(M_1, M_j)}{4} = \max_{1 \leq i \leq L_1 + L_2} \min_{1 \leq j \neq i \leq L_1 + L_2} \frac{\gcd(M_i, M_j)}{4},$$

we can set M_1 as the reference modulus and the error bound $\tau_1 < \min_{1 \leq j \leq L_1 + L_2} \frac{\gcd(M_1, M_j)}{4} = \frac{M}{4}$ in (30).

Then, from (31) when $2 \leq i \leq L_1$, $\tau_i \leq M/2 - M/4 = M/4$; and when $L_1 + 1 \leq i \leq L_1 + L_2$, $\tau_i < MM'/2 - M/4$. So we can accurately determine the folding numbers n_i for $1 \leq i \leq L_1 + L_2$. Next, we can get $\Gamma_{i1} = \frac{M_i}{\gcd(M_1, M_i)} = \Gamma_{1,i}$ for $2 \leq i \leq L_1$ and $\Gamma_{i1} = \Gamma_{2,i}$ for $L_1 + 1 \leq i \leq L_1 + L_2$, all of which are co-prime. Thus, we can obtain a simple closed-form reconstruction formula for \hat{n}_1 similar to (33) and then \hat{n}_i by (22) for $2 \leq i \leq L_1 + L_2$. \blacksquare

Example 2: In the above, let $M = 10, M' = 3, \Gamma_{1,1} = 33, \Gamma_{1,2} = 31, \Gamma_{2,1} = 35, \Gamma_{2,2} = 37$, and the moduli are $\{M_1, M_2, M_3, M_4\} = \{10 \cdot 33, 10 \cdot 31, 30 \cdot 35, 30 \cdot 37\}$. From Corollary 4, we can get $\tau_1 < 10/4$, $\tau_2 \leq 10/4$, $\tau_3 \leq 50/4$, $\tau_4 \leq 50/4$. In addition, it has a closed-form algorithm to robustly reconstruct an unknown integer N for $0 \leq N < \text{lcm}(M_1, M_2, M_3, M_4)$. However, according to the result of [24], the remainder error bounds would be $\tau_1 < 10/4$, $\tau_2 < 10/4$, $\tau_3 < 30/4$, $\tau_4 < 30/4$.

Interestingly, the robustness bound result in this corollary is even better than that obtained in [24] using a two-stage robust CRT. What the result here tells us that for the set of moduli in Corollary 4, which is the set considered in [24], it is not necessary to use a two-stage robust CRT as what is done in [24]. Another remark we make here is that the notation τ_i above denotes the i th remainder error bound. Later, without causing any notational confusion, τ_j will denote the remainder error bound for the remainders in the j -th group.

III. MULTI-STAGE ROBUST CRT

From the study in the previous section, one can see that the robustness bound is kind of dependent on the gcd of the moduli. The larger the gcd is, the better the robustness bound is. However, the large gcd reduces the lcm of the moduli, i.e., reduces the determinable range of the unknown integer N . When a set of moduli are given, the maximal determinable range is given too, which is their lcm. Then, the question is for a given set of moduli, can we improve the robustness bound obtained in Corollary 1? Note that in the single stage robust CRT obtained in the previous section, all the remainders and their related system of congruence equations are considered and solved together simultaneously. A natural question is: can we split the set of moduli into several groups so that the moduli in each group have a large gcd and remainders and their corresponding system of congruence equations in each group are considered and solved independently using the single stage robust CRT obtained in the previous section? If so, can we obtain a better robustness bound than that in Corollary 1 for the single stage robust CRT? To answer these questions, let us first see an example.

Suppose that a set of moduli $\{180, 220, 486, 513\}$ are given and the gcd of these 4 moduli is 1. These four moduli can be split to two groups $\{180, 220\}$ and $\{486, 513\}$. The gcd of the two moduli in the first group is $M = 20$ with $\Gamma_1 = 180/20 = 9, \Gamma_2 = 220/20 = 11$, and the gcd of the two moduli in the second group is $M = 27$ with $\Gamma_1 = 486/27 = 18, \Gamma_2 = 513/27 = 19$. One can see that each group satisfies the condition in Propositions 1

and 2 and therefore the closed-form robust CRT in [13] or the single stage robust CRT in the previous section can be applied for the robust reconstruction of an unknown integer N with robustness bound $\tau < 20/4$ or $\tau < 27/4$, if $N < \text{lcm}\{180, 220\} = 1980 \triangleq q_1 = 18 \cdot 110$ or $N < \text{lcm}\{486, 513\} = 9234 \triangleq q_2 = 18 \cdot 513$, respectively.

Using the first group with moduli $M_1 = 180$ and $M_2 = 220$ and two remainders r_1 and r_2 , if the integer N is in the range of $[0, \text{lcm}(M_1, M_2))$, then N can be uniquely determined by its two error free remainders r_1 and r_2 as N_1 with $0 \leq N_1 < q_1$; otherwise

$$N = N_1 \bmod q_1. \quad (35)$$

Using two erroneous remainders \tilde{r}_1 and \tilde{r}_2 with error level τ , and the closed-form robust CRT in [13] or the single stage robust CRT in the previous section for the first group, we can obtain an integer \hat{N}_1 and

$$\text{if } \tau < \gcd(M_1, M_2)/4 = 20/4, \text{ then } |N_1 - \hat{N}_1| \leq \tau. \quad (36)$$

Similarly, using the second group with moduli $M_3 = 486$ and $M_4 = 513$ and two remainders r_3 and r_4 , if the integer N is in the range of $[0, \text{lcm}(M_3, M_4))$, then N can be uniquely determined by its two error free remainders r_3 and r_4 as N_2 with $0 \leq N_2 < q_2$; otherwise

$$N = N_2 \bmod q_2. \quad (37)$$

Using two erroneous remainders \tilde{r}_3 and \tilde{r}_4 with error level τ , and the closed-form robust CRT in [13] or the single stage robust CRT in the previous section for the second group, we can obtain an integer \hat{N}_2 and

$$\text{if } \tau < \gcd(M_3, M_4)/4 = 27/4, \text{ then } |N_2 - \hat{N}_2| \leq \tau. \quad (38)$$

On the other hand, if integer N is in the range of $[0, \text{lcm}(M_1, M_2, M_3, M_4)) = [0, \text{lcm}(q_1, q_2))$, it can be uniquely determined by its four error free remainders r_1, r_2, r_3, r_4 . This can be done either from the four remainders directly or from the two new remainders N_1 and N_2 of N with two new moduli q_1 and q_2 with equations (35) and (37), respectively. For the robustness, as we mentioned earlier, the closed-form robust CRT and the results in Propositions 1 and 2 can not be applied to the four moduli and the four erroneous remainders directly since they do not satisfy the co-prime condition. In addition, according to our single stage robust CRT in Theorem 1 and Corollary 1 obtained in the previous section, its robustness bound would be $\tau < 9/4$ (interestingly, for the 4 moduli, their gcd is only 1). However, using the above grouping idea, the reconstruction of N can be done in two stages: the first stage is to reconstruct \hat{N}_1 in (36) and \hat{N}_2 in (38) from the two groups, respectively; the second stage is to reconstruct \hat{N} from its two possibly erroneous remainders \hat{N}_1 and \hat{N}_2 with two new moduli q_1 and q_2 . From the second stage, using the known robust CRT again, we obtain

$$\text{if } \tau < \gcd(q_1, q_2)/4 = 18/4, \text{ then, } |N - \hat{N}| \leq \tau. \quad (39)$$

Thus, we have a robust reconstruction too. In order to keep all inequalities (36), (38) and (39), one can see that with this two-stage approach, the robustness bound on the remainder error level τ is $18/4$ which is surprisingly even better than $9/4$ that is the robustness bound in Corollary 1 using the single stage robust CRT for general moduli obtained in the previous section. This means that using two or more groups for a set of moduli may have a better robustness bound than that using a single group for the whole set of moduli. Clearly, for the better robustness, the way to group the moduli or remainders plays a very important role as one can see from the bounds

above. Note that the robustness bound $\tau < 9/4$ in Corollary 1 for the single stage robust CRT for the moduli set $\{180, 220, 486, 513\}$ is only half of the robustness bound $\tau < 18/4$ for the same moduli set $\{180, 220, 486, 513\}$ but with the grouping and the two-stage approach. We next present our results for general cases. First, we consider the case of two groups and two stages.

Let $\{M_{1,1}, M_{1,2}, \dots, M_{1,L_1}, M_{2,1}, M_{2,2}, \dots, M_{2,L_2}\}$ be the whole set of moduli that may not be necessarily all distinct. It is split to two groups with Group 1 of L_1 moduli: $0 < M_{1,1} < M_{1,2} < \dots < M_{1,L_1}$; and Group 2 of L_2 moduli: $0 < M_{2,1} < M_{2,2} < \dots < M_{2,L_2}$. These two groups do not have to be disjoint. Let N be a positive integer, and $r_{1,1}, r_{1,2}, \dots, r_{1,L_1}, r_{2,1}, r_{2,2}, \dots, r_{2,L_2}$ be the corresponding remainders of N , i.e.,

$$N = n_{j,i}M_{j,i} + r_{j,i}, \quad (40)$$

where $0 \leq r_{j,i} < M_{j,i}$ and $n_{j,i}$ is an unknown integer for $1 \leq i \leq L_j$, $j = 1$ or 2 . As we know, N can be uniquely reconstructed from its $L_1 + L_2$ remainders if and only if $0 \leq N < \text{lcm}(\delta_1, \delta_2)$, where $\delta_1 \triangleq \text{lcm}(M_{1,1}, M_{1,2}, \dots, M_{1,L_1})$ and $\delta_2 \triangleq \text{lcm}(M_{2,1}, M_{2,2}, \dots, M_{2,L_2})$. The congruence system (40) can be converted into the following two-stage congruences.

For $j = 1, 2$, and Group j , we can write

$$\begin{cases} N_j = K_{j,i}M_{j,i} + r_{j,i} \\ 0 \leq N_j < \delta_j \\ 1 \leq i \leq L_j. \end{cases} \quad (41)$$

Then, the above N_1 and N_2 can be combined to form a new system of congruences:

$$\begin{cases} N = l_1\delta_1 + N_1 \\ N = l_2\delta_2 + N_2 \\ 0 \leq N < \text{lcm}(\delta_1, \delta_2). \end{cases} \quad (42)$$

When $\delta_1 = \delta_2$, the two congruence equations are degenerated to a single equation and without loss of generality, we assume $\delta_1 \neq \delta_2$ here and such a similar degenerated case is not considered either in what follows in this paper. Replacing N_1 and N_2 in (42) by equations (41), we have

$$\begin{cases} N = l_1\delta_1 + K_{1,i}M_{1,i} + r_{1,i}, & 1 \leq i \leq L_1 \\ N = l_2\delta_2 + K_{2,i}M_{2,i} + r_{2,i}, & 1 \leq i \leq L_2 \\ 0 \leq N < \text{lcm}(\delta_1, \delta_2). \end{cases} \quad (43)$$

It is not hard to see that

$$N = l_j\delta_j + K_{j,i}M_{j,i} + r_{j,i} = (l_j\frac{\delta_j}{M_{j,i}} + K_{j,i})M_{j,i} + r_{j,i},$$

where

$$K_{j,i} < \frac{\delta_j}{M_{j,i}}$$

for $1 \leq i \leq L_j$, $j = 1$ or 2 . Clearly,

$$n_{j,i} = l_j\frac{\delta_j}{M_{j,i}} + K_{j,i}, \quad 1 \leq i \leq L_j, \quad j = 1, 2.$$

From the known values of all the moduli $\{M_{j,i}\}$ and all the erroneous remainders $\{\tilde{r}_{j,i}\}$, if we can accurately determine $K_{j,i}$ and l_j , then we can accurately determine $n_{j,i}$. Thus, we propose the following algorithm to robustly reconstruct N , called two-stage robust CRT, when the remainders are erroneous.

- **Step 1:** Following the single stage robust CRT algorithm of Steps 1-5 in Section II, calculate $\hat{K}_{j,i}$ for $1 \leq i \leq L_j$ in the system of congruence equations (41) from erroneous remainders $\{\tilde{r}_i\}$ for each $j = 1, 2$.
- **Step 2:** After obtaining $\hat{K}_{j,i}$ for $1 \leq i \leq L_j$, $j = 1, 2$, calculate the average estimate \hat{N}_j of N_j for $j = 1, 2$ by equations (3) and (4):

$$\hat{N}_j = \left\lceil \frac{1}{L_j} \sum_{i=1}^{L_j} (\hat{K}_{j,i} M_{j,i} + \tilde{r}_{j,i}) \right\rceil, \quad (44)$$

where $\lceil \cdot \rceil$ stands for the rounding integer (5).

- **Step 3:** Treating \hat{N}_1 and \hat{N}_2 as the new erroneous remainders in the system of congruence equations (42) and following the single stage robust CRT algorithm Steps 1-5 in Section II again, we calculate \hat{l}_1 and \hat{l}_2 .
- **Step 4:** Calculate $\hat{n}_{j,i}$ for $1 \leq i \leq L_j$ and $j = 1, 2$:

$$\hat{n}_{j,i} = \hat{l}_j \frac{\delta_j}{M_{j,i}} + \hat{K}_{j,i}. \quad (45)$$

- **Step 5:** Calculate the average estimate \hat{N} of the unknown integer N :

$$\hat{N} = \left\lceil \frac{1}{L_1 + L_2} \left(\sum_{i=1}^{L_1} (\hat{n}_{1,i} M_{1,i} + \tilde{r}_{1,i}) + \sum_{i=1}^{L_2} (\hat{n}_{2,i} M_{2,i} + \tilde{r}_{2,i}) \right) \right\rceil, \quad (46)$$

where $\lceil \cdot \rceil$ stands for the rounding integer (5).

Then, we have the following result. For $j = 1, 2$, let τ_j denote the error level of the remainders $r_{j,i}$ in the j -th group, i.e.,

$$|\Delta r_{j,i}| = |\tilde{r}_{j,i} - r_{j,i}| \leq \tau_j,$$

for $1 \leq i \leq L_j$ and

$$G_j = \max_{1 \leq i \leq L_j} \min_{1 \leq q \neq i \leq L_j} \frac{\gcd(M_{j,i}, M_{j,q})}{4}.$$

Let

$$G = \frac{\gcd(\delta_1, \delta_2)}{4}.$$

In the above, when the j -th group has only one modulus $M_{j,1}$, then $G_j = \frac{M_{j,1}}{4}$ and the corresponding lcm, δ_j , is just $M_{j,1}$.

Theorem 2: If

$$|\Delta r_{j,i}| \leq \tau_j < \min(G_j, G), \text{ for all } 1 \leq i \leq L_j \text{ and } j = 1, 2, \quad (47)$$

then, we can accurately determine the folding numbers $\hat{n}_{j,i} = n_{j,i}$ for $1 \leq i \leq L_j$, $j = 1, 2$, and the average estimate \hat{N} of the unknown integer N in (46) satisfies

$$|\hat{N} - N| \leq \left\lceil \frac{L_1 \tau_1 + L_2 \tau_2}{L_1 + L_2} \right\rceil, \quad (48)$$

where $\lceil \cdot \rceil$ stands for the rounding integer (5).

Proof: For $j = 1, 2$, according to Corollary 1, when $|\Delta r_{j,i}| \leq \tau_j < G_j$, we can accurately determine $K_{j,i}$ in the systems of congruence equations (41):

$$K_{j,i} = \hat{K}_{j,i}, \text{ for } 1 \leq i \leq L_j. \quad (49)$$

Furthermore, for the average estimates \hat{N}_1 and \hat{N}_2 in (44) in Step 2 above, we have

$$|\Delta N_j| = |N_j - \hat{N}_j| \leq \tau_j,$$

which keeps the same error level as the remainders $r_{j,i}$ for $1 \leq i \leq L_j$, $j = 1, 2$.

In the second stage (42), \hat{N}_1 and \hat{N}_2 become the erroneous remainders. To accurately determine l_1 and l_2 , according to Proposition 2 or Corollary 1, the error levels should satisfy $\tau_1 < G = \frac{\gcd(\delta_1, \delta_2)}{4}$ and $\tau_2 < G = \frac{\gcd(\delta_1, \delta_2)}{4}$, then

$$l_j = \hat{l}_j, \text{ for } j = 1, 2. \quad (50)$$

Thus, combining with the first stage, we have the condition $\tau_1 < \min(G_1, G)$ and $\tau_2 < \min(G_2, G)$ so that $K_{j,i} = \hat{K}_{j,i}$ and $l_j = \hat{l}_j$ for $1 \leq i \leq L_j$, $j = 1, 2$. Namely, we have $n_{j,i} = \hat{n}_{j,i}$ from (45).

After we accurately determine the folding numbers $n_{j,i} = \hat{n}_{j,i}$ for $1 \leq i \leq L_j$, $j = 1, 2$, we can get the average estimate \hat{N} in (46) of the unknown integer N , i.e.,

$$\begin{aligned} \hat{N} &= \left[\frac{1}{L_1 + L_2} \left(\sum_{i=1}^{L_1} (\hat{n}_{1,i} M_{1,i} + \tilde{r}_{1,i}) + \sum_{i=1}^{L_2} (\hat{n}_{2,i} M_{2,i} + \tilde{r}_{2,i}) \right) \right] \\ &= N + \left[\frac{1}{L_1 + L_2} \left(\sum_{i=1}^{L_1} (\Delta r_{1,i}) + \sum_{i=1}^{L_2} (\Delta r_{2,i}) \right) \right]. \end{aligned} \quad (51)$$

From $|\Delta r_{j,i}| \leq \tau_j$ for $1 \leq i \leq L_j$ for $j = 1, 2$, we can easily obtain

$$|\hat{N} - N| \leq \left[\frac{L_1 \tau_1 + L_2 \tau_2}{L_1 + L_2} \right]. \quad (52)$$

Therefore the proof is completed. ■

The above results for two groups of moduli can be easily generalized to a general number of groups of moduli by using Corollary 1 twice for the two stages of the congruence equations as follows.

Assume there are s groups of moduli with $s > 2$. For every $1 \leq j \leq s$, the elements in the j -th group are denoted as $0 < M_{j,1} < M_{j,2} < \dots < M_{j,L_j}$, let $\delta_j \triangleq \text{lcm}(M_{j,1}, M_{j,2}, \dots, M_{j,L_j})$ and τ_j denote the error level of the remainders $r_{j,i}$, $1 \leq i \leq L_j$, from the moduli in the j -th group, and when the j -th group has more than one element, define

$$G_j = \max_{1 \leq i \leq L_j} \min_{1 \leq q \neq i \leq L_j} \frac{\gcd(M_{j,i}, M_{j,q})}{4}. \quad (53)$$

If the j -th group has only one element, $M_{j,1}$, define $G_j = \frac{M_{j,1}}{4}$. Let

$$G = \max_{1 \leq i \leq s} \min_{1 \leq q \neq i \leq s} \frac{\gcd(\delta_i, \delta_q)}{4}. \quad (54)$$

Then, we have the following result.

Theorem 3: If

$$|\Delta r_{j,i}| \leq \tau_j < \min(G_j, G), \text{ for all } 1 \leq i \leq L_j \text{ and } 1 \leq j \leq s, \quad (55)$$

then, we can accurately determine the folding numbers $\hat{n}_{j,i} = n_{j,i}$ for $1 \leq i \leq L_j$ and $1 \leq j \leq s$, thus we can robustly reconstruct \hat{N} as an estimate of N when $0 \leq N < \text{lcm}(\delta_1, \delta_2, \dots, \delta_s)$:

$$\hat{N} = \left[\frac{1}{\sum_{j=1}^s L_j} \sum_{j=1}^s \sum_{i=1}^{L_j} (\hat{n}_{j,i} M_{j,i} + \tilde{r}_{j,i}) \right], \quad (56)$$

and

$$|\hat{N} - N| \leq \left\lceil \frac{\sum_{j=1}^s L_j \tau_j}{\sum_{j=1}^s L_j} \right\rceil. \quad (57)$$

Proof: The proof is similar to the proof of Theorem 2. In the first stage, via (55) we can accurately determine the folding numbers $K_{j,i}$ for $1 \leq i \leq L_j$, $1 \leq j \leq s$, and obtain the robust estimates \hat{N}_j of N_j for the j -th group with the error bound $|\hat{N}_j - N_j| \leq \tau_j < \min(G_j, G)$, where $0 \leq N_j < \delta_j$ for all $1 \leq j \leq s$.

Then, in the second stage we take these estimates \hat{N}_j as erroneous remainders and δ_j as moduli for $1 \leq j \leq s$ to form a new congruence system. Applying the result of Corollary 1 again, we can accurately determine the unknown folding numbers l_j for $1 \leq j \leq s$. By that, we can accurately determine $n_{j,i}$ for $1 \leq i \leq L_j$ with $1 \leq j \leq s$.

Lastly, once we get the accurate values of $n_{j,i}$, the average estimate \hat{N} of N can be found. The error bound of N is proved similar to Theorem 2. Hence, the theorem is proved. \blacksquare

Similar to Corollary 3 for the single stage robust CRT, in the second stage with moduli δ_j and erroneous remainders \hat{N}_j for $1 \leq j \leq s$, we can also individually consider the remainder error level for each remainder \hat{N}_j with respect to modulus δ_j and have the following result.

Corollary 5: Assume that the reference modulus is δ_k for some k with $1 \leq k \leq s$, which satisfies

$$G = \min_{1 \leq q \neq k \leq s} \frac{\gcd(\delta_k, \delta_q)}{4} = \max_{1 \leq i \leq s} \min_{1 \leq q \neq i \leq s} \frac{\gcd(\delta_i, \delta_q)}{4}$$

and its corresponding remainder error bound $\tau_k < G$. If

$$|\Delta r_{k,i}| \leq \tau_k < \min(G_k, G), \text{ for all } 1 \leq i \leq L_k, \quad (58)$$

$$|\Delta r_{j,i}| \leq \tau_j < \min(G_j, \frac{\gcd(\delta_j, \delta_k)}{2} - \min(G_k, G)), \text{ for all } 1 \leq i \leq L_j \text{ and } 1 \leq j \neq k \leq s, \quad (59)$$

then we can accurately determine the folding numbers $\hat{n}_{j,i} = n_{j,i}$ for $1 \leq i \leq L_j$ and $1 \leq j \leq s$.

Example 3: Given three groups of moduli: $\{26 \cdot 5, 26 \cdot 6\}$, $\{27 \cdot 7, 27 \cdot 13\}$, and $\{28 \cdot 15, 28 \cdot 11\}$. We can get $G_1 = 26/4$, $G_2 = 27/4$, $G_3 = 28/4$ and $G = 21/4$. So, from Theorem 3, we obtain the robustness bounds: $\tau_1 < \min(G_1, G) = 21/4$, $\tau_2 < \min(G_2, G) = 21/4$ and $\tau_3 < \min(G_3, G) = 21/4$. If we use the result of Corollary 5, we can get a better error bound for some groups as follows: $\tau_1 \leq 26/4$, $\tau_2 \leq 21/4$ and $\tau_3 < 21/4$.

For a given set of L moduli M_i , $1 \leq i \leq L$, there are many different grouping methods of the remainders, and therefore, many ways to robustly reconstruct the unknown integer from its erroneous remainders. Let us see an example.

Example 4: Consider the moduli set $\{M_1, M_2, M_3, M_4\} = \{48 \cdot 4, 48 \cdot 3, 56 \cdot 3, 56 \cdot 2\}$. First, consider all the moduli as a single group and we obtain the robustness bound $24/4$ according to Corollary 1. Second, we group the four moduli into two groups $\{48 \cdot 4, 48 \cdot 3\}$ and $\{56 \cdot 3, 56 \cdot 2\}$ with $G_1 = 48/4$, $G_2 = 56/4$ and $G = \frac{\gcd(\delta_1, \delta_2)}{4} = 48/4$ in Theorem 2. Accordingly, the robustness bound in this case is $\tau_1 < 48/4$ and $\tau_2 < 48/4$.

Lastly, if we group the four moduli into another two groups $\{48 \cdot 4, 56 \cdot 2\}$ and $\{48 \cdot 3, 56 \cdot 3\}$ with $G_1 = 16/4$, $G_2 = 24/4$ and $G = 336/4$, then, the robustness bound in this case is $\tau_1 < 16/4$ and $\tau_2 < 24/4$.

From this example, we can see that different grouping methods lead to different robustness bounds. Compared with the robustness bound by using a single stage robust CRT for the whole set of moduli, sometimes a grouping can enlarge the robustness bound while sometimes a grouping may decrease the robustness bound. Thus, another question is whether there exists a proper grouping method to ensure the robustness bound larger than that in Corollary 1 using the single stage robust CRT. We next present a result that tells us when there exists a grouping method with a better robustness bound for remainders in some groups using a two-stage robust CRT than that using the single stage robust CRT.

Corollary 6: For a given set of L moduli $\{M_i, i = 1, \dots, L\}$, the robustness bound can not be enlarged for remainders in any group by using a two-stage robust CRT with a grouping method of the moduli if and only if it is the case of [13], i.e., the remaining factors Γ_i of the moduli $M_i = M\Gamma_i$ divided by their gcd M , $1 \leq i \leq L$, are co-prime.

Proof: It is easy to prove the sufficiency as follows. When the moduli M_i satisfy the constraint in [13], i.e., Γ_i are co-prime, its robustness bound using the single stage robust CRT with a single group moduli is $M/4$. On the other hand, from Theorem 3, each G_j of any grouping and G are both $M/4$. Hence, we cannot enlarge the robustness bound in this case.

We next prove the necessity. Assume that the robustness bound for remainders in any group can not be enlarged by the two-stage robust CRT with a grouping method of the moduli over the robustness bound of the single stage robust CRT of the whole set of the moduli. Denote $\gcd(M_i, M_q) = m_{iq}$. Without loss of generality, we can assume

$$\frac{m_{1L}}{4} = \frac{\gcd(M_1, M_L)}{4} = \max_{1 \leq i \leq L} \min_{1 \leq q \neq i \leq L} \frac{\gcd(M_i, M_q)}{4},$$

and

$$m_{12} \geq m_{13} \geq \dots \geq m_{1L}.$$

Thus, according to Corollary 1, its robustness bound using the single stage robust CRT with a single group moduli is $m_{1L}/4$. We then have the following two cases.

Case I: There exists one q with $2 \leq q < L$ such that

$$m_{12} \geq \dots \geq m_{1q} > m_{1(q+1)} \geq \dots \geq m_{1L}.$$

If we group the moduli as Group 1: $\{M_1, \dots, M_q\}$; and Group 2: $\{M_1, M_{q+1}, \dots, M_L\}$. With this grouping, we have that $G_1 > m_{1L}/4$ and $G_2 \geq m_{1L}/4$, $G \geq M/4 > m_{1L}/4$. Thus, we obtain $\tau_1 < \min\{G_1, G\}$, $\tau_2 < \min\{G_2, G\}$, where $\min\{G_1, G\} > m_{1L}/4 = \tau$, which contradicts with the assumption that we cannot enlarge the robustness bound for the remainders in Group 1 using a two-stage robust CRT. This proves that $m_{12} = m_{13} = \dots = m_{1L}$.

Case II: Under the condition of $m_{12} = m_{13} = \dots = m_{1L} = M$, we know that any $m_{iq} = \gcd(M_i, M_q) \geq M$, since M is a factor of all the moduli M_i . Suppose that there exists one $m_{iq} > M$ with $q \neq i \neq 1$. We can group the moduli as Group 1: $\{M_i, M_q\}$, and Group 2: $\{M_i, \{M_{i_1}\}_{i_1 \neq q} \text{ or } i\}$. Similar to Case I, $G_1 > M/4$,

$G_2 \geq M/4$ and $G \geq M_i/4 > M/4$. So, we can enlarge the robustness bound for the remainders in Group 1 by using the two-stage robust CRT with this grouping. This also contradicts with the assumption.

From the above two cases we conclude that $m_{iq} = M$ for all $1 \leq i \neq q \leq L$, i.e., it is the case of [13]. ■

Now, we give an explicit example. Suppose that there are a set of moduli with the form of $\{M_1K_1, M_2K_1, M_2K_2, M_2K_3\}$, where M_1, K_1, K_2, K_3 are co-prime. According to Corollary 1, the robustness bound using the single stage robust CRT is $\tau < \min(M_2, K_1 \gcd(M_1, M_2))/4$. If the moduli are grouped into two groups as $\{M_1K_1, M_2K_1\}$ and $\{M_2K_1, M_2K_2, M_2K_3\}$. Then, according to Theorem 2, its robustness bound is $\tau_1 < K_1 \gcd(M_1, M_2)/4$ and $\tau_2 < M_2/4$, one of which is greater than the robustness bound $\min(M_2, K_1 \gcd(M_1, M_2))/4$ when $M_2 \neq K_1 \gcd(M_1, M_2)$.

Example 5: Let $M_1 = 8$, $M_2 = 14$, $K_1 = 3$, $K_2 = 5$, and $K_3 = 7$. Then we can calculate $\tau_1 < 6/4$ and $\tau_2 < 14/4$ from the two-stage robust CRT. One can see that $\tau_2 < 14/4$ is significantly greater than $\tau < 6/4$ using the single stage robust CRT.

From Corollary 6, one can see that as long as Γ_i in moduli M_i are not all co-prime, using a two-stage robust CRT with some grouping method has a larger robustness bound for remainders in some groups than the single stage robust CRT does. In the same way, we may treat $\{\delta_1, \delta_2, \dots, \delta_s\}$ as a new set of moduli and group it again so that the single stage robust CRT is applied three times with the following result. We call it three-stage robust CRT.

Let us split $\{\delta_1, \delta_2, \dots, \delta_s\}$ in Theorem 3 to k groups. For every $1 \leq t \leq k$, the elements in the t -th group are denoted as $0 < \delta_{t,1} < \dots < \delta_{t,y_t}$, let $\xi_t \triangleq \text{lcm}(\delta_{t,1}, \dots, \delta_{t,y_t})$ and define

$$\Upsilon_t = \max_{1 \leq i \leq y_t} \min_{1 \leq q \neq i \leq y_t} \frac{\gcd(\delta_{t,i}, \delta_{t,q})}{4}.$$

Let

$$\Upsilon = \max_{1 \leq i \leq k} \min_{1 \leq q \neq i \leq k} \frac{\gcd(\xi_i, \xi_q)}{4}.$$

We then have the following result.

Theorem 4: If

$$|\triangle r_{j,i}| \leq \tau_j < \min(G_j, \min_t \{\Upsilon_t : \delta_j \in \{\delta_{t,1}, \dots, \delta_{t,y_t}\}\}, \Upsilon), \text{ for all } 1 \leq i \leq L_j, 1 \leq j \leq s \text{ and } 1 \leq t \leq k, \quad (60)$$

then, we can accurately determine the folding numbers $\hat{n}_{j,i} = n_{j,i}$ for $1 \leq i \leq L_j$ and $1 \leq j \leq s$, thus we can robustly reconstruct \hat{N} as an estimate of N when $0 \leq N < \text{lcm}(\delta_1, \delta_2, \dots, \delta_s)$:

$$\hat{N} = \left[\frac{1}{\sum_{j=1}^s L_j} \sum_{j=1}^s \sum_{i=1}^{L_j} (\hat{n}_{j,i} M_{j,i} + \tilde{r}_{j,i}) \right], \quad (61)$$

and

$$|\hat{N} - N| \leq \left[\frac{\sum_{j=1}^s L_j \tau_j}{\sum_{j=1}^s L_j} \right]. \quad (62)$$

Proof: The congruence system

$$N = n_{j,i} M_{j,i} + r_{j,i},$$

where $0 \leq r_{j,i} < M_{j,i}$ for $1 \leq i \leq L_j$, $1 \leq j \leq s$ and $0 \leq N < \text{lcm}(\delta_1, \delta_2, \dots, \delta_s)$, can be converted into the following three-stage congruences.

For $1 \leq j \leq s$, and Group j in the first stage, we can write

$$\begin{cases} N_j = K_{j,i}M_{j,i} + r_{j,i} \\ 0 \leq N_j < \delta_j \\ 1 \leq i \leq L_j. \end{cases} \quad (63)$$

In the second stage,

$$\begin{cases} P_t = H_{t,i}\delta_{t,i} + N_{t,i} \\ 0 \leq P_t < \xi_t \\ 1 \leq i \leq y_t \\ 1 \leq t \leq k. \end{cases} \quad (64)$$

Then, in the third stage, we can write

$$\begin{cases} N = l_t\xi_t + P_t \\ 0 \leq N < \text{lcm}(\xi_1, \dots, \xi_k) \\ 1 \leq t \leq k. \end{cases} \quad (65)$$

As long as we can accurately determine all of $K_{j,i}$, $H_{t,i}$ and l_t in each congruence system, we can then accurately determine $n_{j,i}$. According to conditions (60), we can accurately determine $K_{j,i}$ for $1 \leq i \leq L_j$, $1 \leq j \leq s$ and get the error bound

$$|\hat{N}_j - N_j| \leq \tau_j < \min(G_j, \min_t \{\Upsilon_t : \delta_j \in \{\delta_{t,1}, \dots, \delta_{t,y_t}\}\}, \Upsilon).$$

Next, in each group of the second stage we take these estimates \hat{N}_j as erroneous remainders and δ_j as moduli. Applying the result of Corollary 1, we can accurately determine $H_{t,i}$, and also get the robust estimate \hat{P}_t satisfying

$$|\hat{P}_t - P_t| < \min(G_j, \min_t \{\Upsilon_t : \delta_j \in \{\delta_{t,1}, \dots, \delta_{t,y_t}\}\}, \Upsilon).$$

Similarly, treat the estimates \hat{P}_t as the erroneous remainders and ξ_t as moduli in the third stage. Since $|\hat{P}_t - P_t| < \Upsilon$, from Corollary 1 again, we can accurately determine l_t . Once we accurately determine these unknown folding numbers in each congruence system, we can accurately determine $n_{j,i}$ and then obtain the robust estimate \hat{N} of the unknown integer N . As for the error bound of the estimate \hat{N} , the proof is the same to that of Theorem 2. Therefore, we complete the proof. \blacksquare

Example 6: Consider a given set of moduli $\{96 \cdot 2, 96 \cdot 3, 72 \cdot 3, 72 \cdot 5, 64 \cdot 5, 64 \cdot 7\}$. Treating them as one group and using the single robust CRT, we get its error bound τ for the remainders satisfying $\tau < 32/4$. If we split the moduli to three groups: $\{96 \cdot 2, 96 \cdot 3\}$, $\{72 \cdot 3, 72 \cdot 5\}$ and $\{64 \cdot 5, 64 \cdot 7\}$, we get $G_1 = 96/4$, $G_2 = 72/4$, $G_3 = 64/4$, $\delta_1 = 96 \cdot 2 \cdot 3$, $\delta_2 = 72 \cdot 3 \cdot 5$, $\delta_3 = 64 \cdot 5 \cdot 7$ and $G = 64/4$. By using the two-stage robust CRT, we can get the error bounds τ_j for the remainders in Group j for $j = 1, 2, 3$ satisfying $\tau_1 < \min(G_1, G) = 64/4$, $\tau_2 < \min(G_2, G) = 64/4$ and $\tau_3 < \min(G_3, G) = 64/4$, all of which are larger than the bound $32/4$ in the single robust CRT. If we use the three-stage robust CRT and split $\{\delta_1, \delta_2, \delta_3\}$ to two groups again: $\{\delta_1, \delta_2\}$ and $\{\delta_3\}$. We can get $\Upsilon_1 = 72/4$, $\Upsilon = 320/4$. So, in this three-stage robust CRT, the error bounds satisfy $\tau_1 < \min(G_1, \Upsilon_1, \Upsilon) = 72/4$, $\tau_2 < \min(G_2, \Upsilon_1, \Upsilon) = 72/4$ and $\tau_3 < \min(G_3, \Upsilon) = 64/4$. Compared with the two-stage robust CRT, we increase the robustness bounds in Group 1 and Group 2 from $64/4$ to $72/4$ by using the three-stage robust CRT.

The above three-stage robust CRT can be easily generalized to a multi-stage robust CRT with more than three stages. Although we can use a multi-stage robust CRT with some grouping methods to obtain a larger robustness bound for remainders in some groups, there are some challenges about how to choose moduli in a group and how many groups and stages we should split in order to find a better robustness bound such that we can enlarge all the robustness bounds in every group.

Let us first look at the simplest case when there are only three moduli $\{M_1, M_2, M_3\}$. Without loss of generality, we can assume that $\gcd(M_1, M_2) \geq \gcd(M_1, M_3) \geq \gcd(M_2, M_3)$. Regarding the three moduli as one group and by Corollary 1, the robustness bound is $\gcd(M_1, M_3)/4$. Since $\gcd(M_3, M_2) \leq \gcd(M_3, M_1)$, if we want to obtain a robustness bound strictly larger than $\gcd(M_1, M_3)/4$, the modulus M_3 must independently form an individual group by itself, and in the meantime it does not allow other groups to include M_3 . Thus, there is only one possible grouping method as $\{M_3\}$ and $\{M_1, M_2\}$. The robustness bound therein is $\tau_1 < \gcd(M_3, \text{lcm}(M_1, M_2))/4$ and $\tau_2 < \min(\gcd(M_1, M_2), \gcd(M_3, \text{lcm}(M_1, M_2)))/4$, which may be both larger than $\gcd(M_1, M_3)/4$. Otherwise, we have to group them as $\{M_1, M_3\}$ and $\{M_1, M_2\}$ and in this way we may only enlarge one group's (not all group's) robustness bound as what is used in the proof of Corollary 6.

Example 7: When $M_1 = 560$, $M_2 = 480$ and $M_3 = 210$, we can see that $\gcd(M_1, M_2) = \gcd(560, 480) = 80$, $\gcd(M_1, M_3) = \gcd(560, 210) = 70$ and $\gcd(M_2, M_3) = \gcd(480, 210) = 30$. Regarding these three moduli as a single group, the robustness bound of the single stage robust CRT is $\gcd(M_1, M_3)/4 = \gcd(560, 210)/4 = 70/4$. In order to find a larger robustness bound, we just only consider the robustness bound of the case of two groups: $\{M_3\}$ and $\{M_1, M_2\}$. We can get $\tau_1 < 210/4$ and $\tau_2 < 80/4$, which are all larger than $70/4$.

The above special case is about only three moduli's grouping. When the number of given moduli is larger, it becomes more complicated. In the next section, we analyze some special cases.

IV. AN ALGORITHM FOR GROUPING MODULI IN TWO-STAGE ROBUST CRT

From the above study, one may see that for a given set of moduli, although its determinable range for an integer from its remainders is fixed, i.e., the lcm of all the moduli, the robustness bounds for an erroneous remainder and a reconstructed integer depend on a reconstruction algorithm from erroneous remainders, which depends on the grouping of the moduli in a multi-stage robust CRT. For a general set of moduli, it is not obvious on how to group them in a multi-stage (or even two-stage) robust CRT, in particular when the number of moduli is not small. In this section, based on Theorem 3 for the two-stage robust CRT, we propose an algorithm for grouping a general set of moduli to possibly obtain a larger robustness bound for remainders in every group than that in Corollary 1 for the single stage robust CRT.

For a given set of moduli $\mathcal{M} = \{M_1, M_2, \dots, M_L\}$, $L \geq 3$, we first assume that the set of moduli does not include any pair of M_{i_1} and M_{i_2} satisfying $M_{i_1} = nM_{i_2}$, because Corollary 2 has told us that such a redundant modulus M_{i_2} does not help to increase the determinable range of N , $0 \leq N < \text{lcm}(M_1, M_2, \dots, M_L)$ nor the robustness bound in a single stage robust CRT. From condition (55) we need to assure that all G_j in (53) and G in (54) after a grouping strictly greater than $\Theta \triangleq \max_{1 \leq i \leq L} \min_{1 \leq j \neq i \leq L} \frac{\gcd(M_i, M_j)}{4}$ in Corollary 1 for the single stage robust CRT. Then, we have an algorithm as follows.

- 1) For each M_i , $1 \leq i \leq L$, find all M_j , $1 \leq j \neq i \leq L$, satisfying $\frac{\gcd(M_i, M_j)}{4} > \Theta$. With M_i , form the

corresponding set \mathcal{M}_i :

$$\mathcal{M}_i = \{M_i, M_j : \frac{\gcd(M_j, M_i)}{4} > \Theta\}.$$

Thus, with each set \mathcal{M}_i , we have

$$G_i \geq \min_{M_j \in \mathcal{M}_i} \frac{\gcd(M_j, M_i)}{4} > \Theta.$$

If modulus M_i satisfies $\frac{\gcd(M_j, M_i)}{4} \leq \Theta$ for all M_j , $1 \leq j \neq i \leq L$, then we let $\mathcal{M}_i = \{M_i\}$.

- 2) Among all of the L sets \mathcal{M}_i for $1 \leq i \leq L$, there may be one or more pairs, \mathcal{M}_{i_1} and \mathcal{M}_{i_2} , satisfying $\mathcal{M}_{i_1} \subseteq \mathcal{M}_{i_2}$. In this case, we can delete the smaller set \mathcal{M}_{i_1} and only keep the larger set \mathcal{M}_{i_2} .
- 3) After Step 2), from the remaining sets of $\{\mathcal{M}_i\}$, we find all such combinations of $\{\mathcal{M}_{i_1}, \mathcal{M}_{i_2}, \dots, \mathcal{M}_{i_l}\}$ that $\bigcup_{j=1}^l \mathcal{M}_{i_j}$ exactly includes all moduli \mathcal{M} . In other words, if anyone \mathcal{M}_{i_s} for $1 \leq s \leq l$ is deleted from a combination $\{\mathcal{M}_{i_1}, \mathcal{M}_{i_2}, \dots, \mathcal{M}_{i_l}\}$, then $\bigcup_{j=1 \& j \neq s}^l \mathcal{M}_{i_j}$ is a proper subset of \mathcal{M} , i.e.,

$$\mathcal{M} \neq \bigcup_{j=1 \& j \neq s}^l \mathcal{M}_{i_j} \subset \mathcal{M} \subseteq \bigcup_{j=1}^l \mathcal{M}_{i_j}. \quad (66)$$

- 4) As for every combination in the above, treat each \mathcal{M}_{i_j} as a small group and calculate its lcm as δ_{i_j} , $1 \leq j \leq l$. Then, check whether

$$G = \max_{1 \leq p \leq l} \min_{1 \leq q \neq p \leq l} \frac{\gcd(\delta_{i_p}, \delta_{i_q})}{4} > \Theta. \quad (67)$$

If there is one combination $\{\mathcal{M}_{i_j}\}$ as above to make inequality (67) hold, then every $\min(G_{i_j}, G)$, $1 \leq j \leq l$, is strictly greater than Θ . According to (55) in Theorem 3, one can see that this combination is just a grouping as desired and it enlarges a robustness bound for remainders in every group by using the two-stage robust CRT. Otherwise, if for every possible combination in Step 3), inequality (67) does not hold, then it is said that we fail to use this algorithm to enlarge a robustness bound for remainders in every group by using the two-stage robust CRT.

Let us first consider the above grouping algorithm for the case of [13], i.e., the remaining factors Γ_i of the moduli $M_i = M\Gamma_i$ divided by their gcd M , $1 \leq i \leq L$, are co-prime. First, we find all $\mathcal{M}_i = \{M_i\}$, $1 \leq i \leq L$. Next, there is only one combination $\{\mathcal{M}_1, \mathcal{M}_2, \dots, \mathcal{M}_L\}$ satisfying (66), and we treat each $\mathcal{M}_i = \{M_i\}$ as one group, then calculate $G = M/4$ in (67), which equals to $\Theta = M/4$. In conclusion, we fail to find a grouping to enlarge a robustness bound for remainders in every group by using the two-stage robust CRT, which can be also confirmed from the earlier result in Corollary 6. Next, we give a positive example.

Example 8: Consider a set of moduli $\{210M, 143M, 77M, 128M, 81M, 125M, 169M\}$, where M is an integer. As one group, using the single stage robust CRT, its robustness bound is $\Theta = M/4$. According to the above grouping algorithm, find 7 sets: $\mathcal{M}_1 = \{210M, 77M, 128M, 81M, 125M\}$, $\mathcal{M}_2 = \{143M, 77M, 169M\}$, $\mathcal{M}_3 = \{77M, 210M, 143M\}$, $\mathcal{M}_4 = \{128M, 210M\}$, $\mathcal{M}_5 = \{81M, 210M\}$, $\mathcal{M}_6 = \{125M, 210M\}$ and $\mathcal{M}_7 = \{169M, 143M\}$. Among them, there are only four combinations satisfying (66) as follows: $\{\mathcal{M}_1, \mathcal{M}_2\}$, $\{\mathcal{M}_1, \mathcal{M}_7\}$, $\{\mathcal{M}_2, \mathcal{M}_4, \mathcal{M}_5, \mathcal{M}_6\}$ and $\{\mathcal{M}_3, \mathcal{M}_4, \mathcal{M}_5, \mathcal{M}_6, \mathcal{M}_7\}$. Then, check whether one of the above four combinations satisfies inequality (67). Fortunately, for the first combination $\{\mathcal{M}_1, \mathcal{M}_2\}$, inequality (67) holds.

We can calculate $G_1 = 2M/4$, $G_2 = 11M/4$ and $G = 7M/4$, all of which are strictly greater than $M/4$. Thus, we have obtained a grouping method of the moduli to enlarge a robustness bound for remainders in every group by using the two-stage robust CRT.

Remark 2: As one can see in the proof of Corollary 6 and in the above algorithm and examples, a modulus M_i may be repeatedly used in more than one groups in the two-stage robust CRT. Its aim is to make G and G_j after grouping greater than or equal to the robustness bound by using the single stage robust CRT for the whole set of moduli. Recall the case of grouping a set of three moduli $\{M_1, M_2, M_3\}$. Assume $\gcd(M_1, M_2) > \gcd(M_1, M_3) > \gcd(M_2, M_3)$. From Corollary 1, the robustness bound for using the single robust CRT is $\frac{\gcd(M_1, M_3)}{4}$. According to the above grouping moduli algorithm in two-stage robust CRT, they are split to two groups: $\{M_1, M_2\}$ and $\{M_3\}$. One can see that $G_1 = \frac{\gcd(M_1, M_2)}{4}$, $G_2 = \frac{M_3}{4}$, $\delta_1 = \text{lcm}(M_1, M_2)$, $\delta_2 = M_3$ and $G = \frac{\gcd(\delta_1, \delta_2)}{4}$. In this grouping method, the robustness bound for remainders in group $\{M_1, M_2\}$ is $\min(G_1, G)$ and the robustness bound for remainders in group $\{M_3\}$ is $\min(G_2, G)$. As G_1 and G_2 are greater than $\frac{\gcd(M_1, M_3)}{4}$, a robustness bound for remainders in each group depends on the value of G . When $G = \frac{\gcd(\delta_1, \delta_2)}{4}$ is less than $\frac{\gcd(M_1, M_3)}{4}$, a robustness bound for remainders in each group is worse than that for the single robust CRT. Thus, we should repeat modulus M_1 in group $\{M_3\}$, and the two groups become $\{M_1, M_2\}$ and $\{M_1, M_3\}$. In this way, we enlarge a robustness bound for group $\{M_1, M_2\}$ and keep the robustness bound for group $\{M_1, M_3\}$ non-changed. On the other hand, when $G = \frac{\gcd(\delta_1, \delta_2)}{4}$ is larger than $\frac{\gcd(M_1, M_3)}{4}$, we do not need to repeat modulus M_1 , since the robustness bound for group $\{M_1, M_2\}$ and the robustness bound for group $\{M_3\}$ are both greater than $\frac{\gcd(M_1, M_3)}{4}$. This example tells us that, to enlarge the robustness bound, whether a modulus M_i is repeatedly used or not in multiple groups depends on the grouping method and the set of moduli. Repeating a modulus, sometimes, may help to enlarge the robustness bound but sometimes may not.

V. SIMULATIONS

In this section, we present some simple simulation results to evaluate the proposed single stage robust CRT algorithm and the two-stage robust CRT algorithm for integers with a general set of moduli. Let us first consider the case when $M_1 = 9 \cdot 15$, $M_2 = 9 \cdot 20$ and $M_3 = 9 \cdot 18$. These three moduli do not satisfy the condition that Γ_i , $i = 1, 2, 3$, are co-prime and thus the robust CRT obtained in [12], [13] can not be applied directly. However, we can use our proposed single stage robust CRT. According to Corollary 1, the maximal range of the determinable N is 1620 and the maximal remainder error level τ for the robustness is upper bounded by $\tau < \frac{27}{4}$ from (27). In this simulation, the unknown integer N is uniformly distributed in the interval $[0, 1620)$. We consider the maximal remainder error levels $\tau = 0, 1, 2, 3, 4, 5, 6$, and the errors are also uniformly distributed on $[0, \tau]$ in the remainders. 2000000 trials for each of them are implemented. The mean error $E(|\hat{N} - N|)$ between the estimated \hat{N} in (4) and the true N is plotted by the solid line marked with \square , and the theoretical estimation error upper bound in (6) is plotted by the solid line marked with \triangle in Fig. 1. Obviously, one can see that for a general set of moduli the reconstruction errors of N from the erroneous remainders are small compared to the range of N .

Next, we compare the robustness between the single stage and the two-stage robust CRT algorithms for the above same set of moduli. In this case, the conditions of the maximal remainder error levels for the single stage and the two-stage robust CRT algorithms of two groups $\{M_1, M_2\}$ and $\{M_3\}$ are $\frac{27}{4}$ and $\frac{45}{4}$, i.e., $\tau \leq 6$ and

11, respectively. Let us consider the maximal remainder error levels τ from 0 to 25, and 2000000 trials for each of them. The unknown integer N is taken as before. Fig. 2 shows the curves of the error bounds and the mean estimation errors $E(|\hat{N} - N|)$ for both the single stage and the two-stage robust CRT algorithms. Note that from our single stage robust CRT theory, the valid error bound for τ is only upto 6, which can be seen from the simulation results that the mean estimation error $E(|\hat{N} - N|)$ starts to deviate the previous line trend at $\tau = 7$, then increases significantly and breaks the linear error bound when τ is further greater, i.e., robust reconstruction may not hold. On the other hand, with the two-stage robust CRT algorithm, one can see that the curve of the mean estimation error $E(|\hat{N} - N|)$ is always below the curve of the error bound, i.e., we can robustly reconstruct N , $0 \leq N < 1620$, even when the maximal error level is 11 that is the upper bound for τ obtained in this paper for the two-stage robust CRT algorithm. These simulation results confirm the theory obtained in this paper.

VI. CONCLUSION

In this paper, we considered the robust reconstruction problem from erroneous remainders, namely robust CRT problem, for a general set of moduli that may not satisfy the condition needed in the previous robust CRT studies in [12], [13]. We obtained a necessary and sufficiency condition for the robust CRT when all the erroneous remainders are used together, called single stage robust CRT. Interestingly, our proposed single stage robust CRT may have better robustness than that of the robust CRT obtained in [12], [13] even when it could be applied. To further improve the robustness, we then proposed a multi-stage robust CRT, where the moduli are grouped into several groups. As an example, for the two-stage robust CRT, our proposed single stage robust CRT is first applied to each group and then applied across the groups second time. Also, an algorithm on how to group a given set of moduli was proposed. We finally presented some simulations to verify our proposed theory.

REFERENCES

- [1] J. H. McClellan and C. M. Rader, *Number Theory in Digital Signal Processing*, Englewood Cliffs, NJ: Prentice-Hall, 1979.
- [2] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, Singapore: World Scientific, 1999.
- [3] O. Ore, "The general Chinese remainder theorem," *Amer. Math. Monthly*, vol. 59, no. 6, pp. 365-370, Jun.-Jul. 1952.
- [4] Y. Wang, "New Chinese remainder theorems, in *Proc. The Thirty-Second Asilomar Conference on Signals, System and Computer*, pp. 165-171, Asilomar, Pacific Grove, CA, Nov. 1998.
- [5] O. Goldreich, D. Ron, and M. Sudan, "Chinese remaindering with errors," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 1330-1338, Jul. 2000.
- [6] V. Guruswami, A. Sahai, and M. Sudan, "Soft-decision decoding of Chinese remainder codes," in *Proc. 41st IEEE Symp. Foundations Computer Science*, Redondo Beach, CA, 2000, pp. 159-168.
- [7] I. E. Shparlinski and R. Steinfeld, "Noisy Chinese remaindering in the Lee norm," *J. Complex.*, vol. 20, pp. 423-437, 2004.
- [8] X.-G. Xia, "Estimation of multiple frequencies in undersampled complex valued waveforms," *IEEE Trans. Signal Process.*, vol. 47, pp. 3417-3419, Dec. 1999.
- [9] X.-G. Xia and K. Liu, "A generalized Chinese remainder theorem for residue sets with errors and its application in frequency determination from multiple sensors with low sampling rates," *IEEE Signal Process. Lett.*, vol. 12, pp. 768-771, Nov. 2005.
- [10] Z. Huang and Z. Wan, "Range ambiguity resolution in multiple PRF pulse Doppler radars," in *Proc. Int. Conf. Acoustics, Speech, Signal Process. (ICASSP)*, pp. 1786-1789, Dallas, TX, Apr. 1987.

- [11] X.-G. Xia and G. Wang, "Phase unwrapping and a robust Chinese remainder theorem," *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 247-250, Apr. 2007.
- [12] X. W. Li, H. Liang, and X.-G. Xia, "A Robust Chinese remainder theorem with its applications in frequency estimation from undersampled waveforms," *IEEE Trans. Signal Process.*, vol. 57, no. 11, pp. 4314-4322, Nov. 2009.
- [13] W.-J. Wang and X.-G. Xia, "A Closed-form robust Chinese remainder theorem and its performance analysis," *IEEE Trans. Signal Process.*, vol. 58, no. 11, pp. 5655-5666, Nov. 2010.
- [14] W. Xu, E. C. Chang, L. K. Kwok, H. Lim, and W. C. A. Heng, "Phase unwrapping of SAR interferogram with multi-frequency or multi-baseline," in *Proc. IGARSS*, 1994, pp. 730-732.
- [15] D. P. Jorgensen, T. R. Shepherd, and A. S. Goldstein, "A dual-pulse repetition frequency scheme for mitigating velocity ambiguities of the NOAA P-3 airborne Doppler radar," *J. Atmos. Ocean. Technol.*, vol. 17, no. 5, pp. 585-594, May 2000.
- [16] G. Wang, X.-G. Xia, V. C. Chen, and R. L. Fiedler, "Detection, location, and imaging of fast moving targets using multifrequency antenna array SAR," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 40, no. 1, pp. 345-355, Jan. 2004.
- [17] M. Ruegg, E. Meier, and D. Nuesch, "Capabilities of dual-frequency millimeter wave SAR with monopulse processing for ground moving target indication," *IEEE Trans. Geosci. Remote Sens.*, vol. 45, no. 3, pp. 539-553, Mar. 2007.
- [18] Y. M. Zhang and M. Amin, "MIMO radar exploiting narrowband frequency-hopping waveforms," in *Proc. 16th European Signal Processing Conference (EUSIPCO 2008)*, Lausanne, Switzerland, August 25-29, 2008.
- [19] J. Bioucas-Dias, V. Katkovnik, J. Astola, and K. Egiazarian, "Multi-frequency phase unwrapping from noisy data: adaptive local maximum likelihood approach," book chapter in *Image Analysis, Lecture Notes in Computer Science*, vol. 5575/2009, pp. 310-320, Jul. 2009.
- [20] W.-K. Qi, Y.-W. Dang, and W.-D. Yu, "Deblurring velocity ambiguity of distributed space-borne SAR based on Chinese remainder theorem," *J. Electron. & Inform. Tech.*, vol. 31, no. 10, pp. 2493-2496, Oct. 2009.
- [21] G. Li, H. Meng, X.-G. Xia, and Y.-N. Peng, "Range and velocity estimation of moving targets using multiple stepped-frequency pulse trains," *Sensors*, vol. 8, pp. 1343-1350, 2008.
- [22] G. Li, J. Xu, Y.-N. Peng, and X.-G. Xia, "Location and imaging of moving targets using non-uniform linear antenna array," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 43, no. 3, pp. 1214-1220, Jul. 2007.
- [23] X. W. Li and X.-G. Xia, "Location and imaging of elevated moving target using multi-frequency velocity SAR with cross-track interferometry," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 47, no. 2, pp. 1203-1212, Apr. 2011.
- [24] B. Yang, W. J. Wang, Q. Yin, and X.-G. Xia, "Phase detection based range estimation with a dual-band robust Chinese remainder theorem," preprint, 2013.
- [25] W. C. Li, X. Z. Wang, X. M. Wang, and B. Moran, "Distance estimation using wrapped phase measurements in noise," *IEEE Trans. Signal Process.*, doi: 10.1109/TSP.2013.2238934, downloadable via IEEE Explore, 2013.

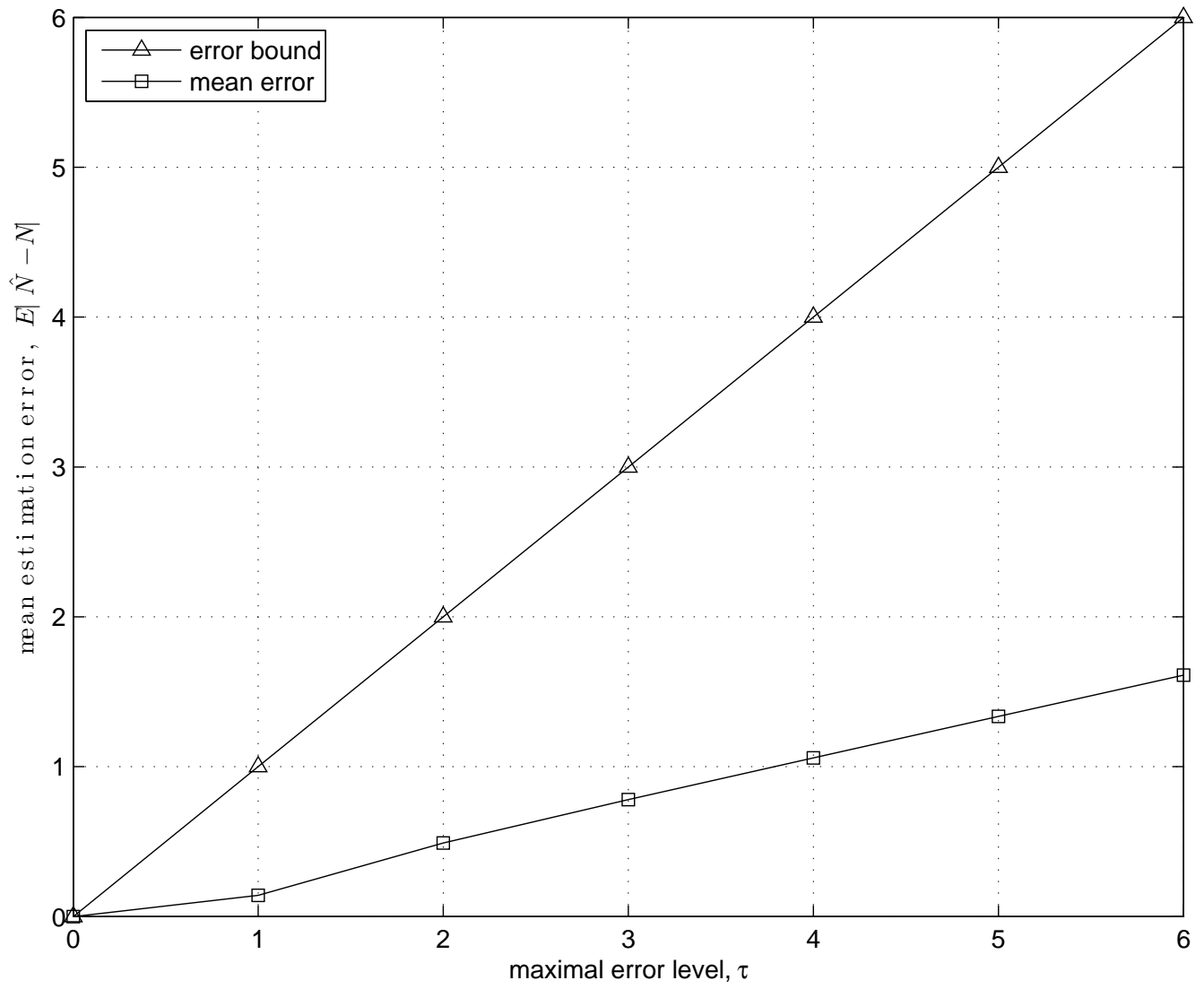


Fig. 1. Mean estimation error and theoretical error bound using the single stage robust CRT

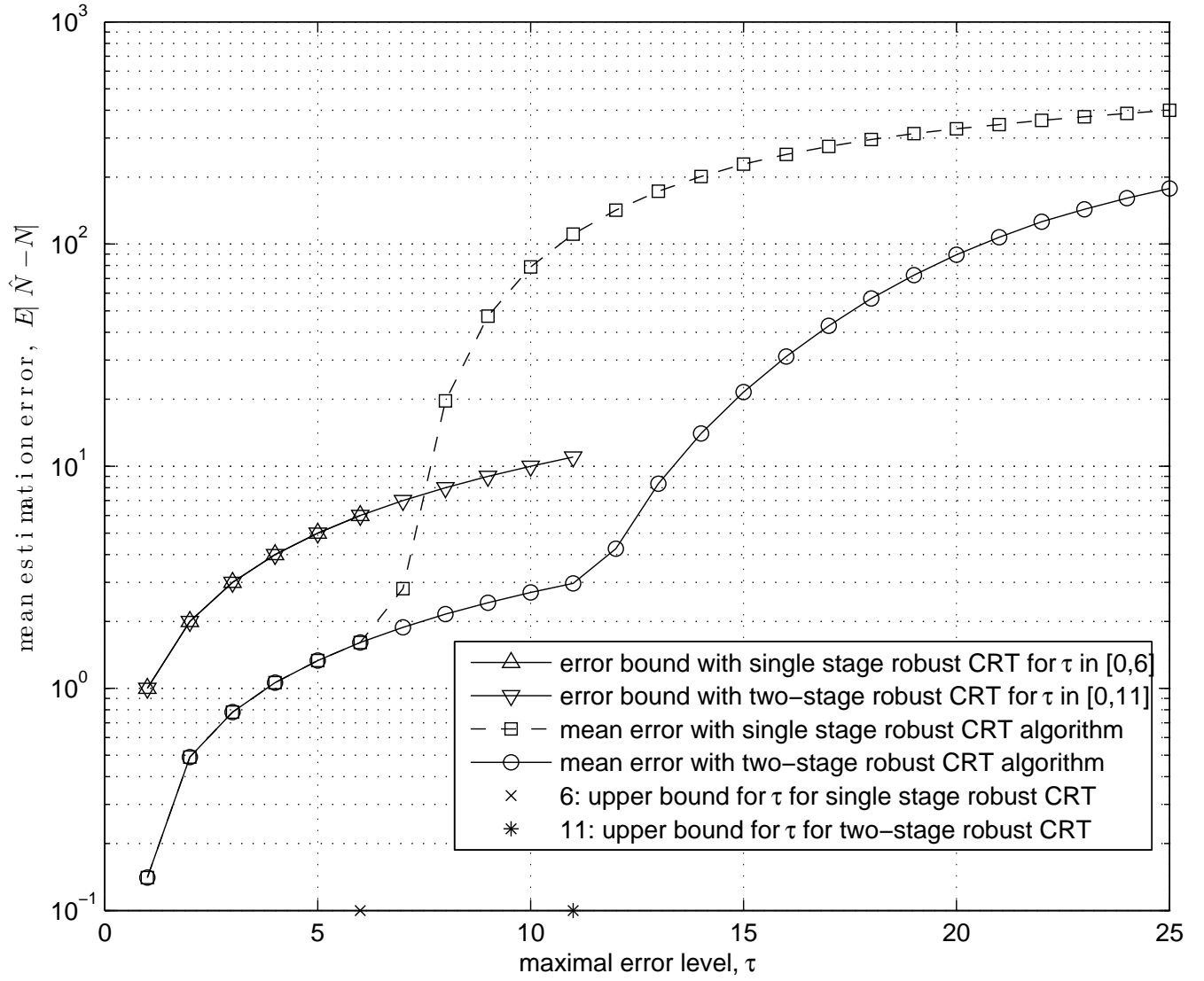


Fig. 2. Mean estimation error and theoretical error bound comparison using the single stage robust CRT and the two-stage robust CRT